

# ODISCYE

## Online Disinformation and Cyber Insecurities in International Politics

---

Lucas M. Schubert

International Politics and Conflict Studies  
Faculty of Social Sciences  
University of the Bundeswehr Munich



# Table of Contents



## 1. Executive Summary



## 2. Disinformation and (In-)Securities as old/long-standing security phenomena



## 3. Introduction to **online disinformation** and cyber insecurities taxonomy and terminology



## 4. **Online disinformation and cyber insecurities:** international frameworks and regulations



## 5. How do **international online disinformation and cyber-attacks** affect and threaten Germany, the EU and NATO?



## 6. **Has the digital dragon awakened?** The People's Republic of China and its plan to become a cyberworld power



## 7. **The Russian Federation:** information warfare and cyber sabotage – “designated battlefields” as understood by Moscow



## 8. **Big Tech** – Obscure Friends



## 9. **State of Play:** How do Germany, the EU, NATO and global initiatives aim to challenge international online disinformation and cyber insecurities



## 10. **Way ahead:** Examination of the cyber strategies and policy suggestions for EU, NATO, Germany and the global level

## EDITORIAL

### Dear Reader,

The 21st century is already 23 years old, and in many ways things are turbulent, hectic and uncertain due to a breathtaking technological revolution, based on the Internet, that we are currently witnessing.

Just 20 years ago, e-commerce, online learning, and the Internet of Things (IoT) were either unknown, still in their infancy, or ridiculed as mere gimmicks that would never take off. Hacking was considered an ominous, scary fringe phenomenon, a subculture that no one really understood.

The Internet has long since grown far beyond being a mere gimmick; it has become critical infrastructure. It is an indispensable part of our modern civilization; without it, healthcare, government administration, research and the maintenance of public safety but also daily interaction, for example, would no longer be possible.

But with all the possibilities, came dangers, such as managed disinformation, fake news, identity and data theft, cyber espionage, digital attacks on vital points of entire countries, such as electricity and water supplies, and the ever-present threat of a possible surveillance and police state through the back door. These are just a few negative aspects of our not-so-new digital society. As is so often the case, however, social and political development is lagging behind technological development, which is currently taking giant steps and also threatens to run away from us. In society, new manners and institutions must first be renegotiated again and again; this circumstance naturally slows down the ability to react, but it is nevertheless necessary.

Russia's brutal war against Ukraine, China's nationalist turn during the last few years and challenges by both powers against the liberal international order are a contextual element that has to be taken extremely serious when addressing online disinformation and cyber insecurities. And so is the need to counter these threats resolutely, while maintaining – and indeed improving – a rule-based international order in which self-determination, human rights and the inadmissibility of aggression have to be fostered, regionally and globally. More research and discussion are needed to accelerate this process. With this ODISCYE Policy Compendium you hold in your hands a contribution to this debate, containing knowledge and recommendations, for decision makers in politics, military, business and



Prof. Dr. Stephan Stetter, ODISCYE Head of Project, Institute of Political Science, University of the Bundeswehr Munich

academia, but also for any individual interested in this subject area.

It is the result of three years of research, as well as a conference with distinguished experts from the fields of computer sciences, political science, military, international relations, sociology and economics, who pro-

*"Nothing is more powerful than an idea whose time has come."*

Victor Hugo

professionally deal with cyber security and online disinformation. Further, I want to proudly mention, that a paper by my research associates Anna Reuss, M.A. and Lucas Maximilian Schubert, M.A. related to the mentioned topics received the *Early Career Researcher Award* during a NATO STO Conference last year in Stockholm. You will find a link to it in the book.

I would like to take this opportunity to thank them all. But most of all I wish to thank Lucas Schubert for the excellent and devoted work on this project and this very policy compendium. Many thanks also to the Bundeswehr Centre for Public Affairs for generously supporting this project.

A complete list of all who contributed to this project can be found below.

It remains for me to wish you an enjoyable read, I hope you find new, valuable and insightful Food for Thought.

Yours,  
Prof. Dr. Stephan Stetter  
Head of the ODISCYE Project



# 1 Executive Summary

---

**Disinformation** in the information environment is the deliberately planned attempt to spread uncertainty and insecurity in the discourse of a group perceived as antagonistic or hostile, via digital technology.

**Internet of Things** describes the fact that more and more everyday objects are connected to the Internet. This opens pathways to sabotage more and more fundamentally “material” objects today through the detached technological possibilities of the Internet.

**Cyberattacks** are a modern form of sabotage that connect the offline and online worlds.

Cybercrime in the narrow sense means the use of a computer as a weapon to obtain goods without permission.

Acquiring financial assets in an unlawful way through a computer

- By individuals or organized crime

Cyber espionage is the effort of intelligence agencies to obtain information on the Internet through means of infiltration that are not publicly available. It can be carried out directly by government bodies, but also by hacking-for-hire and so-called “patriotic hackers” to cover tracks.

- Achieve unauthorized access
- Obtain classified information

Cybersabotage uses acquired knowledge and access from cyber espionage to cause targeted damage to foreign systems. It is discussed in more detail in the terminology on cybersecurity and in the points on individual scenarios and states.

- Disruption of routines at an adversary
- Make processes impossible
- Corrupt data

Cyberwar is any attack by computer-based means on a country's critical infrastructure. It is a means, in the

context of which no immediate diplomatic solution is sought, and instead optioning for a “solution” to address geopolitical questions with warlike means.

- Destruction or disabling of Critical Infrastructure of an adversary

► Cyber crime is often a necessary condition for successful actions in the field of espionage, but the difference between pure cybercrime and cyber espionage are the motives and the perpetrators.

**Attribution** – the distinction between cyber sabotage and cyber war already begins with the detection of traces indicating authorship. However, it is often hard to determine exactly who is responsible for an attack, because certain groups or even state actors also use their own specific programs and have their own specific approaches to attacks.

## Cyberthreats

Cyber threats are manifold and can affect infrastructure, machines, the economy and important social processes.

### 1. Power Infrastructure (Electrical Energy)

The energy supply represents the lifeline of every developed country, without it no production, water supply, health care, traffic control, or communication is possible.

A functioning power supply is vital for Germany's security. A highly complex, elaborate and sophisticated generation, control and supply structure is used, which is connected via the Internet and is therefore a weak point for possible hacker attacks.

A widespread loss of electricity of just under three days is enough to bring the country to the brink of collapse. Hospitals would have fuel only for a few days to run emergency generators, and food would become scarce after a week.

## 2. Supply Chains

The complex and highly technological production methods of German industry and commerce depend on smooth processes and deliveries. Nowadays, logistics, orders, inventories and deadline processing are managed, recorded and handled electronically. An interruption of these by hackers, for example, can paralyze production times with a just-in-time model and cause irreparable damage.

## 3. Military, economic, and intelligence motivated Cyber Espionage

Germany is a country of innovation; without scientific, inventive and thus also economic progress, the country is not in a position to be among the leading players in international competition. Admittedly, players such as China no longer rely on stealing innovations directly; they now have excellent developers themselves. However, key technologies are still being researched in which, for example, they still have a unique position, such as modern adhesives. Efforts are also being made to find out where weaknesses exist in the “adversaries” systems, how quickly the defenses react and what is being planned.

## 4. State administration, democratic structures, E-Governance, confidential personal data

Personal data of citizens, such as social security data, foremost health data (medical data sets e.g.), tax office data, law enforcement data and other confidential information are the focus of hackers. In addition, personal profiles on social media are in the crosshairs. However, also documents of parliamentarians, investigative committees and personal information about them are in the crosshairs of cyberattacks.

## 5. Online Disinformation and Fake News

Contrary to widespread opinion, unfortunately often conveyed in this way by the media, online disinformation does not attempt to build up new patterns of opinion. That would be far too ambitious and costly. Rather, it exploits social frictions and an already battered debate culture in society and tries to widen these fissures. It seeks to create the impression that the entire state is corrupt and beyond salvation, and that the government is actively fighting its own citizens.

Online disinformation uses every trick in the book: News is either fabricated (fake news), or actual information is distorted in an alienated context, videos are deceptively faked, fake accounts are used to simulate a high level of approval for content and spread it.

## China

The leadership in Beijing wants to become a great power and establish a hegemony in East Asia. This includes an intensification of information warfare.

Beijing made it clear that a new cybersecurity strategy is being developed, based on three pillars:

- expanding cyber military and warfare capabilities
- limiting the threat of the internet to Beijing’s hold on power which extends to domestic information control
- shaping global cyberspace norms to extend China’s influence

This strategy is directly linked to the expansion of the People’s Liberation Army’s military clout in the field of active cyber warfare.

Six years ago, the People’s Liberation Army was drastically reformed, and a new Strategic Support Force was created. It has competencies in space warfare, political warfare, electronic warfare, and cyber warfare.

The People’s Republic of China does not speak of “hybrid conflicts” or “cyberwarfare”, but of “informationized conflicts”.

Beijing’s Network Systems Department has its own state-owned company that produces hardware and software in the fields of communications technology and data processing for civilian and military applications. This makes it much more difficult for Beijing to prevent foreign espionage attempts that target technological vulnerabilities.

A pillar of the strategy is the securitization and standardization of the legal framework for commercial data in the People’s Republic of China. This gives Beijing the ability to access, monitor and control commercial data at any time and thus exert pressure.

## Policy Recommendations

The Chinese authorities force companies to use Chinese codes and tools if they want to do business in China, the same rule can be applied to European law if Chinese companies want to do business in the EU.

Strengthening intelligence capabilities in the area of active source hunting and information gathering is necessary, as well as improved technological analysis of attacks.

*“We live in a pivotal era and may not even realize it. An unknown land lies ahead of us. The digital age has dawned and we must set the course to protect our freedom and the democracy we live in without being afraid of progress.”*

Lucas Maximilian Schubert, M.A.,  
ODISCYE Research Associate,  
University of the Bundeswehr Munich



Corporate management should strengthen employees' sensitivity to the trustworthiness of data and keep suspicious code detection programs up to date. Companies should establish a shared confidential database to share information regarding suspicious activities, stolen codes, forged security certificates, etc.

## Russia

Russia actively uses digital measures to influence public opinion in various countries, has already deployed parts of its arsenal in the military field for cyber sabotage in the ongoing war against Ukraine, and is a global actor in cyberspace.

The foreign policy of the Russian Federation is understood in a permanent threat situation by the European Union, NATO and the USA. This legitimizes, in the view of Moscow, the use of extreme means in the area of armed forces, intelligence services and diplomacy.

A comprehensive surveillance and censorship program was initially launched against the country's own population, but was later applied to the Internet. The latest version of the technology, SORM-3, also documents all social media channels.

The GRU is the military intelligence service of the Russian armed forces, and is now officially called the Main

Administration of the General Staff of the Armed Forces of the Russian Federation.

### ■ Unit 54777

This unit is engaged in “psychological warfare”, which includes placing targeted disinformation in states perceived as “hostile” in order to “influence public opinion,” according to widespread notions. Another target group is the Russian-speaking diaspora abroad.

### ■ Unit 26165

Also known as “Fancy Bear,” “Strontium,” and “APT 28” conducts cyberattacks on the digital infrastructure and resources of “hostile states” and seeks to achieve financial, structural, and technological damage.

### ■ Unit 74455

Also known as “Sandworm” deals with the professionalized theft of information, as was evident in the course of the 2016 US-presidential election.

### Internet Research Agency (IRA)

The IRA conducts most of the operations, that is a para-state organization that is privately owned, and creates structures that persist over a long time-span. It follows the rulebook of active measures, the paradigm of Soviet and now Russian intelligence. The IRA is parts of a much larger Russian state-funded, military-civilian cyber-network called “Vulkan”.

*“For me as a Computer Scientist, it was very important to exchange on the topic of cybersecurity with people who are not from my field of expertise, to see the problem through their eyes and to think outside the box.”*

Prof. Dr. Georg Groh, Computer Scientist,  
Technical University of Munich (TUM)



### Policy Recommendations

Online disinformation is a challenge that is not easy to master. The misconception that online disinformation is simply lies must be abandoned, and information must be soberly analyzed for the deliberate misinterpretation, linkage, and contextualization by Russian propaganda units.

Digital literacy is still in its infancy in the European Union. Users often consume online content uncritically and only read content that underscores and reinforces their already existing opinions.

The European Union and NATO nations must agree on a unified and centralized approach to reporting, analyzing, and preventing hacking attacks on critical infrastructure.

### EU Policy Recommendations:

#### 1. No legislation is better than bad legislation

Innovation and digital literacy will be the driving forces of the future. Educated citizens, who are aware of technical features, their functions, implications, usage and limits are the cornerstone of the new digital society. A climate of trust and security has to be established through unified and simple solution-oriented approaches.

##### ► Many different sizes fit all

There is no option to meet the needs of all participants (industry, civil society, etc.) in just one law (One size fits all).

##### ► Legal Certainty

Bad legislation has one of the most dangerous consequences: Uncertainty. Citizens, but as well businesses

will reduce their activity or implement very restrictive terms of use, to avoid any collusion with the law and possible consequences.

##### ► Regain trust through good practice in law and low compliance costs

##### ► No Mushrooming of new agencies

Multiple parallel structures which might stand within an unhealthy relationship of competition do not solve problems, but produce more of them.

### 2. Protection of innovative activity

Small and medium software development companies are the motor of European digital industries. They should benefit from tax exemptions to reduce costs, to keep the European market fit for international competition, as well to make the EU interesting for founders and investors.

► The EU should make use of its financial power and create software and innovation centers to ensure that it is on top edge of new development and innovation processes in the field. In terms of technology investment and innovation beats regulation

### Big Tech needs accountability not backdoors

##### ► Enhance transparency and accountability

Mandate increased transparency from Big Tech corporations regarding their algorithms, data practices, and content moderation policies to ensure they can be held accountable. This can help protect civil rights such as freedom of expression while curbing misinformation and discriminatory content.



## NATO Policy Recommendations:

### 1. Keep analogue systems as crisis backup

► Even though modernization, that is digitalization proceeds and is inevitable, “old” forms of defense communications and reconnaissance technology should be kept maintained and ready

► It is wise to invest time and assets in teaching young military personnel in the usage of the “obsolete” technology, in order to have it up and ready in any case

### 2. Keep Nuclear Weapons strictly off the grid

► All systems for command, control, aiming, launching and service of nuclear weapons has to be kept off the digital grid at all costs

### 3. Develop Cyber Diplomacy

► Establish a “Red Smartphone”

In analogy to the “Red Telephone” from the Cold War between Washington and Moscow there should be a fast lane for crisis communication between the major international blocks of power concerning cybersecurity issues, especially cyberattacks.



Prof. Dr. Florian Muhle, Media Sociologist, Zeppelin University Friedrichshafen



Quo vadis digital society and security? Snapshot from one of the panels at the ODISCYE expert workshop (Dr. Liebetrau, Prof. Dr. Stetter, Prof. Dr. Gohdes, Schultze, M.A. and Dr. Reinhold)



Insights from the insiders. Snapshot from another panel at the ODISCYE expert workshop in Berlin, 2022. (Dr. Gaycken, Isik, Prof. Dr. Groh, Prof. Dr. Gallwitz, Dr. King)



Where is the digital world headed to? ODSICYE expert workshop at the Bundeswehr Cyber Innovation Hub (CIH) in Berlin, June, 27th – 28th 2022

#### **4. Counter Disinformation with public awareness and openness to criticism**

► Meet cognitive warfare methods like psyops and disruption with rebuilding trust among the civilian population. Seek out direct contact with citizens and their questions, treat the population as partners and allies in a collective readiness to defend freedom and democracy.

#### **Germany Policy Recommendations**

##### **1. Accelerate digitalization**

► There is no excuse for black spots on the map. In some regions in Germany there is still neither a reliable internet connection nor network reception. This slows the country down in its economic, academic and civil development

##### **2. Improve digital literacy of the general population**

► Use state funds to make schools nutrient soil for cyber resilience

Basic, mid and higher education have to integrate mandatory courses in internet privacy, security and good practice. Community colleges have to increase their offer in effective courses for internet security and data handling.

#### **3. Stop Big Brother in its wake – Make governmental bodies independent and accountable**

► Responsible Disclosure

It has to be mandatory for the BSI to report security gaps and detected backdoors immediately and transparent. All participants and stakeholders in the internet can work then on a solution to fix it.

► Take advantage of the swarm...

Responsible disclosure can activate the entire internet community to work on a solution for a certain security gap.

► ...but hold the developer responsible

Software companies should be obliged to fix security breaches in their code. If necessary, even punishable with a fine to ensure compliance.

#### **4. Use Open Source code for critical infrastructure**

► Keep it stored

Open Source solutions can be stored by institutions in order to have them ready to create a fast solution

► Enable the Federal Agency for Technical Relief (THW) to have the capacities to aid in digital cases of emergency, this would ensure a reliable, unbureaucratic and swift reaction to security breaches. The digital sphere is just another part of critical civilian infrastructure, and such it should be taken care of by well organized professionals that are financed by the public

**5. Constructive dialogue, transparency and openness for debate instead of biased fact checking**

► Like in the recommendation for NATO, it is crucial to expose own mistakes and work on improving the situation. Disinformation loses its own scandalous and disrupting edge if it is shown, that there might be sometimes a true fact in it, just depicted in a very distorted way. It is no shame to speak about own failures, it is a shame trying to cover them up

Both Germany and the EU should finally, strive for international debate at G20, UN and other levels to tackle, through soft and hard international law and diplomatic understandings, online disinformation and

cyber insecurity. International rules and regulations should protect liberal democracy and also offer ideas how core tenets of liberal democracy – freedom of expression, individual liberty, limits to state authority – can be ensured in the internet age.



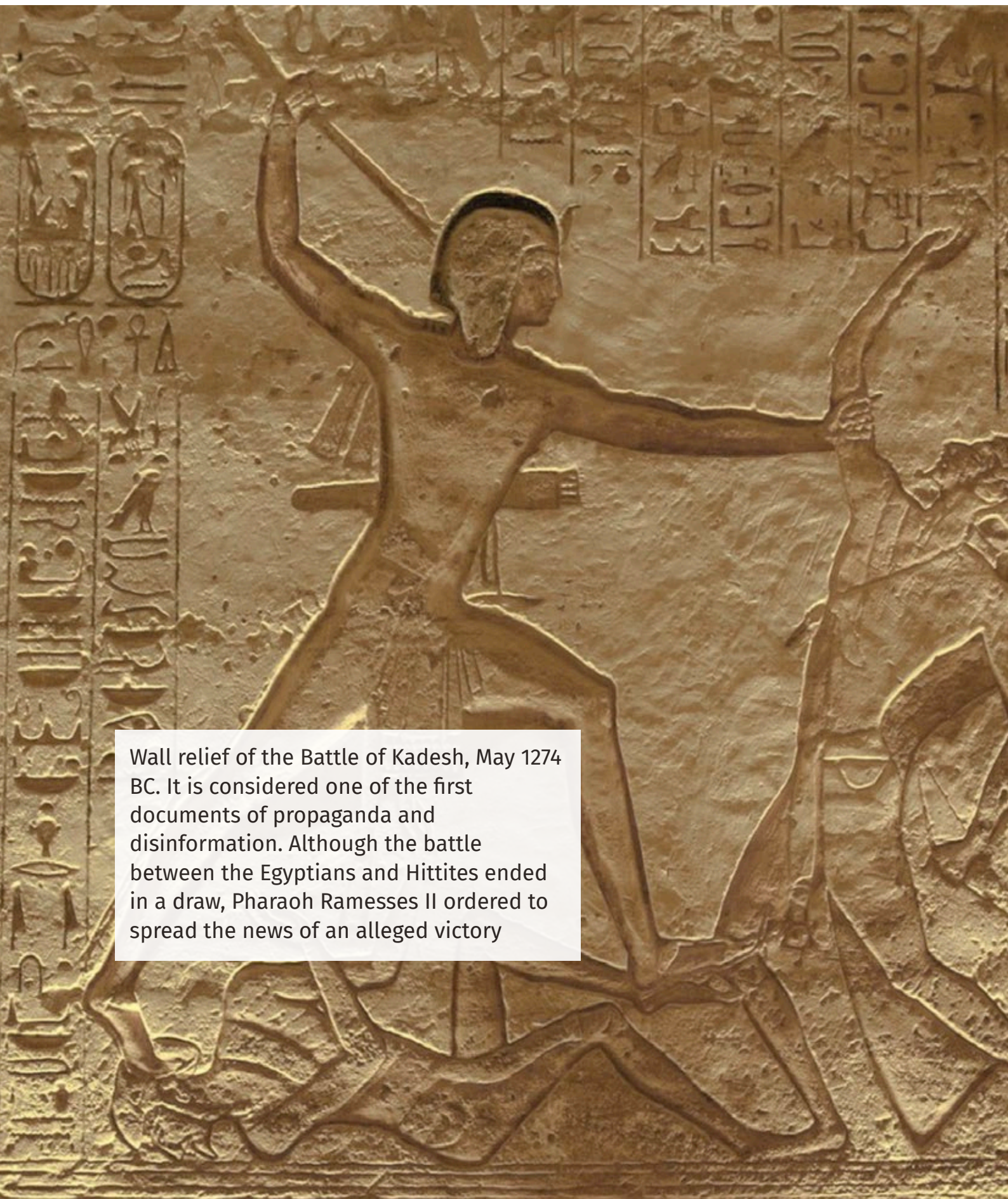
Andrea Garcia Rodriguez, Lead Digital Policy Analyst, European Policy Centre (CEP)



Dr. Ross King, Computer Scientist, Austrian Institute of Technology (AIT)



Deep into the web – working atmosphere during the ODISCYE expert workshop at the Bundeswehr Cyber Innovation Hub (CIH) in Berlin, June, 27th – 28th 2022



Wall relief of the Battle of Kadesh, May 1274 BC. It is considered one of the first documents of propaganda and disinformation. Although the battle between the Egyptians and Hittites ended in a draw, Pharaoh Ramesses II ordered to spread the news of an alleged victory

2

# Disinformation and (In-)Securities as old/long-standing security phenomena

### In a nutshell

- Disinformation and Sabotage are no new phenomena, but as old as human history
- The novelty of online disinformation and cyber threats is their easier and faster availability for a growing number of actors with a wider area of effect and their novel technological nature which renders both offensive and defensive operations a novel field with little learning lessons so far acquired
- Both online disinformation and cyber attacks are one of the major security challenges for Germany, the EU and NATO

They are currently on everyone's lips – **online disinformation and cybersecurity threats**, and some terms are also circulating again and again in connection with them: deep fakes, social bot networks, hacking, critical infrastructure, leaks, or even blackout.

This study intends to discuss the extent to which cyberattacks, cyber espionage and online disinformation affect Germany, the EU and NATO. This is because online disinformation and cyberattacks represent a security problem for the liberal democratic order, at the national and supranational levels and the level of the alliance, that cannot be ignored. While online disinformation is an attempt to deepen divisions in society and promote political polarization, we deal with cyber attacks with the attempt to paralyze and destroy the critical infrastructure of society. This means the lifelines of societies: electric power, water supply, data security, and defense. In the course of this report, we will not only discuss the structures and possible dan-

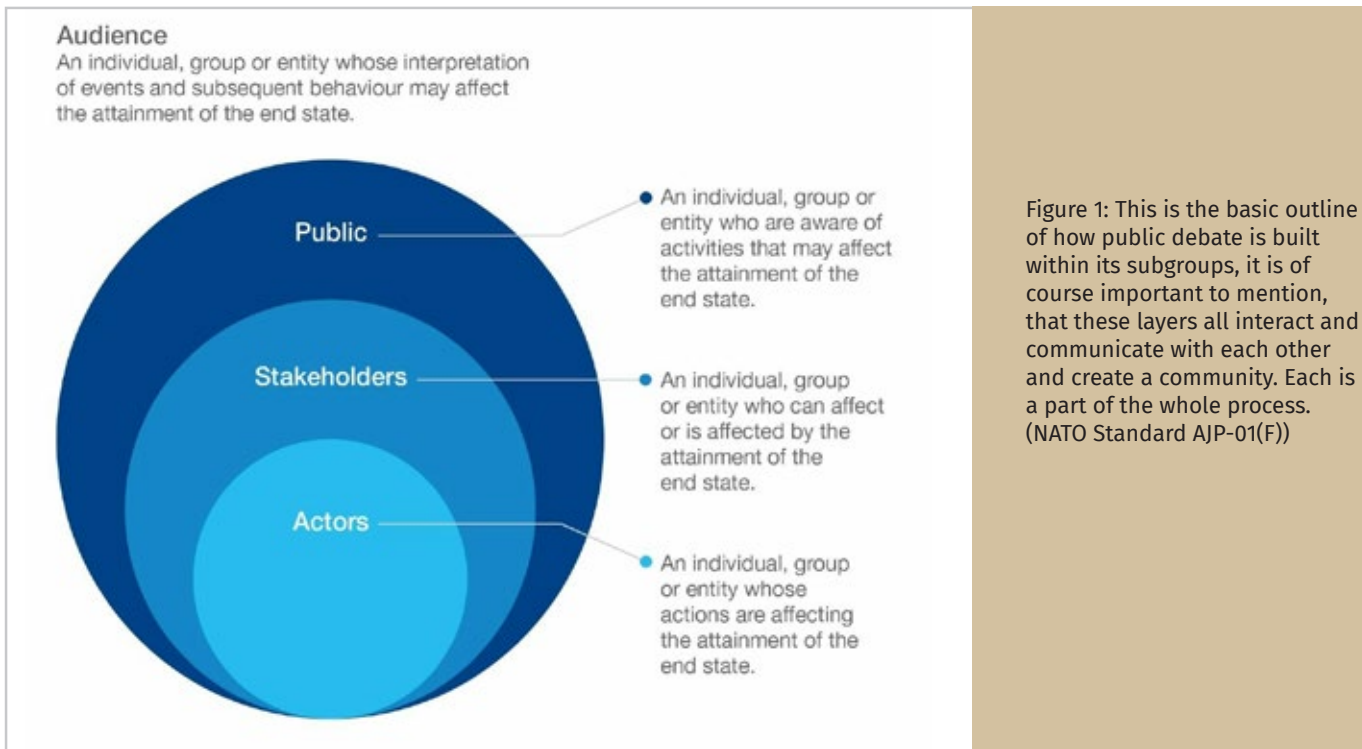
gers, but also possible measures to be able to defend against such threats – but also critically discuss the relevance of counterstrategies.

Many people are uneasy about the threatening scenarios associated with cyberspace. There is a lot at stake. Public security, personal data, the freedom to form independent opinions, or even the continued existence of liberal democracy and the liberal, rule-based multilateral order.

This unease is compounded by the fact that these are techniques in the realm of the Internet. As such, they are abstract and not exactly comprehensible to many; after all, not everyone is a programmer. This is the common perception.

However, this is only partially true. Although these problems are of course new to national security because of the modern technology they use, the underlying principles are not new at all.

Disinformation and propaganda are in fact incredibly old phenomena and have accompanied the history of mankind since the beginning of historiography. One of the first provable cases of state propaganda is, for example, the battle of Kadesh, 1285 B.C. In that case, the Egyptian ruling caste of the time had a version spread and artistically designed, which had hardly anything to do with the actual events. According to this version, Ramses II was the radiant victor who captured Kadesh and crushed his enemies, the Hittites. From stelae, walls and papyri, in songs and stories, this version was conveyed to the people. In truth, the battle



ended in a draw at best. However, that was not important; what was important was the identity-forming myth for ancient Egypt.

Basically, nothing has changed in this approach to this day. Only the technical possibilities have changed over the centuries, at times drastically as with the invention of book printing in the mid-15th century CE and then the invention of the Internet in the late 20th century. As a result, propaganda and disinformation can be spread more rapidly and reach more people across larger distances in shorter time more subtly than was previously the case. But already here a distinction must be made: strictly speaking, propaganda and disinformation are not the same thing.

Propaganda aims to influence public opinion on a broad scale. US political scientist Harold Lasswell, a pioneer of propaganda research in the early 20th century, stated that propaganda is the deliberate influencing of the ideas of third parties by a group, with fixed objectives, using psychological manipulation. What is striking about this definition is the characteristic that the background is irrelevant here. Strictly speaking, advertising, election campaigns, membership drives of associations and company descriptions are also propaganda.

In essence, disinformation in the information environment is the deliberately planned attempt to spread uncertainty and insecurity in the discourse of a group perceived as antagonistic or hostile, with the aim of neutralizing the resilience, cohesion, and integrity of that group, via digital technology. Although always destructive and malicious, it is not always false information: it can be true information disseminated by mixing kernels of truth with manipulated interpretations. Hence, it is most of the time based on the toxic mixing of distorted truths and twisted interpretations.

Today, leaflets are only used in rare situations. And to place complicated fake news reports in hardcopy newspapers or TV news is nowadays almost superfluous. What is needed today is, somewhat casually, a few motivated and trained employees with stable Internet access and Twitter accounts, located somewhere on the globe. The target groups can be reached worldwide at any time, the web finds its way into almost every corner, and the message is heard and spreads quickly.

**Unlike with cyberattacks, in online propaganda and disinformation technology only serves as a vector, i.e., a gateway, to spread the messages. It is a sufficient condition, but not a necessary one. The situation is quite different in the case of security risks in the area of cyberattacks.**

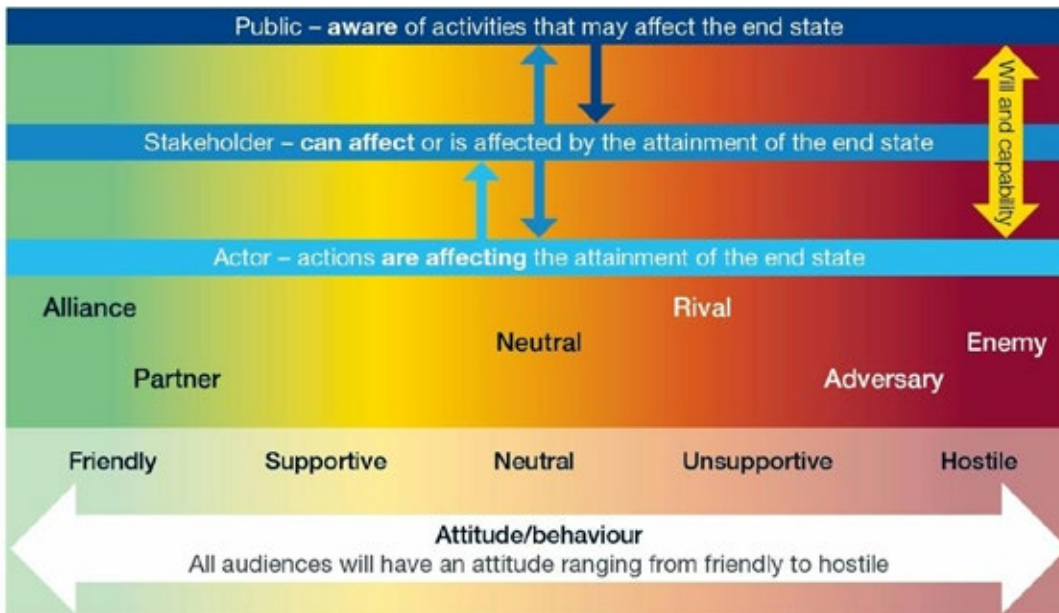


Figure 2: Online Disinformation tries to deepen the rift on both sides of the spectrum of supportive and unsupportive attitudes (NATO STANDARD AJP-01(F))

These have the central aspect of technology, because they aim to cause damage in the online world, but also in the offline world, through deliberately planned, automated or manual manipulation of devices and software. There are a variety of ways to do this, which also involve a many technical terms that may be incomprehensible to laypersons. However, there is also a historical reference that can be made here: sabotage.

The term sabotage probably originates from the 19th century, when French workers, staging early class protest against harsh work conditions, put their heavy wooden shoes into the machines to bring them to a standstill. The reason was a protest against the advancing mechanization of work and the resulting fear of unemployment. As we can see, sabotage in most cases has a political dimension, but it targets technical devices.

What makes cyberattacks, a modern form of sabotage, “new” is the strong connection between the offline and online worlds. Cyberattacks are, thus, best understood as not only a digital phenomenon but rather as the interface between the digital and the material. The Internet is the largest human-made artificial structure that has ever existed. Already, more information is believed to exist inside the WWW than outside it, according to the Australian start-up Health IT the amount of information in the net exceeds 64 zettabytes, which is 64 trillion gigabytes. As information, we understand all knowledge that exists in the form of text, data, communication and audiovisual material. A

recurring term that should be mentioned right here is the “*Internet of Things*” (IoT):

Internet of Things describes the fact that more and more everyday objects are connected to the Internet. Not only industrial machines, but now also central heating systems, refrigerators and washing machines can be maintained and controlled via the Internet. The state administration is not only connected to the worldwide network but also obtains information via various servers and has various e-governance offerings. Power plants of electric utilities are also interconnected by computers communicating via WWW. In short, this opens pathways to sabotage more and more fundamentally “material” objects today through the detached technological possibilities of the Internet. You no longer need strike brigades and lots of clogs, but all you theoretically need is expertise and a working laptop – and sabotage from a distance.

### Snapshots

We would like to illustrate some examples of online disinformation and cyber attacks. This is to briefly highlight the range and types of these phenomena and give you an idea of what is currently being done.

### Online Disinformation

One may be surprised, because some of the examples given here might be familiar to careful observers of political life. Yet, often these examples are not,

wrongly, referred to as disinformation. But it is precisely then when disinformation has achieved its goal, because it is only successful if it has not been recognized as such and has found its way into the debate space. Once there, it is almost impossible to remove it again.

### The Coronavirus as a Chinese Bioweapon

After the Covid 19 pandemic swept the world, people searched for answers as to how this global catastrophe could have occurred. A culprit was sought, and an Indian international relations journal, *Great Game India*, thought it had found evidence that the People's Republic of China was behind it<sup>1</sup>. The latter had stolen a prototype of the virus from a Canadian laboratory, converted it into an operational bioweapon and put it into circulation. The motive was Beijing's attempt to increase its own global influence by subsequently making a vaccine available. This sounds like an explosive, coherent narrative, but there is one problem: it is completely fictitious. Nevertheless, this and many more versions of this story circulated on social media as well, and even today, suspicions remain with many people. The importance of a **coherent and self-contained narrative** for the success of online disinformation will be discussed in the following chapters.

### Vladimir Putin – leader of the free world, with a gigantic fan base?

In April 2022, just a short time after Russia began its invasion of Ukraine, thousands of posts appeared in pro-Kremlin groups on Facebook hailing the Russian president. 650,000 people alone seemed to agree that Vladimir Putin was a great leader who defended the “free world” against the “corrupt and imperialist West”.<sup>2</sup> Within these groups there was a lively interaction on these postings, it looked like many people agreed with the statements and there was indeed a large support scene in the world for the Russian war of aggression. At a superficial glance, this appearance might even be true, yet it was a matter of cleverly contrived “*astroturfing*”. The accounts of the claqueurs were all fake, they were not real persons but so-called bots, automated or semi-automated programs. Russian intelligence services had created them and simulated an entire debate. We will come back to this later.



In the Bundeswehr Cyber Innovation Hub team, servicemen and women, reservists and civilian employees all pull together.

### The Ghost of Kiev

Shortly after the Russian army invaded its neighboring country Ukraine, the news circulated in Western media as well: a daring and talented Ukrainian pilot had shot down dozens of Russian fighter jets over the skies of Kiev. On social networks, the news went “viral” as they say, meaning it spread extremely fast and journalists started to pick it up. The only problem with this story: the ghost of Kiev never existed. Although even the former president of Ukraine, Poroshenko, spread tweets about the alleged pilot, he never existed at any time. To this day, it is not entirely clear who exactly spread this disinformation. For laymen, however, it was not obvious whether the story was true or not. The associated video clip was a montage with content from the computer game “Digital Combat Simulator” and was ultimately also spread by the social media profiles of the Ukrainian army<sup>3</sup>. This is a so-called “*deepfake*”, a term that will play an important role in this study.





## Cyberattacks

### The Stuxnet attacks – software causes real, physical damage

In 2011, the public only became aware of a new type of computer virus, the so-called “Stuxnet worm”, by chance. Some antivirus software companies had detected it on several servers, however, to their amazement, it did not actively cause any damage to the systems. What they were not aware of at the time was the target of the malware: a specific software configuration in the uranium enrichment centrifuges of the Iranian nuclear program. The spread and transmission was quite slow, via the Internet and eventually via infected USB sticks. Yet Stuxnet reached its target address. About 10% of the corresponding equipment at Iran’s Natanz was destroyed by the virus through a targeted change in the rotation speed of the centrifuges. Although this only led to short-term delays in the work of the enrichment factories, it was nevertheless the

first time that large-scale technology in the “real” world had been attacked. To this day, it can only be guessed who exactly was behind this attack. Israel, the U.S., or even a collaboration of both with an industrial company have been suspected, but each side denies responsibility to this day<sup>4</sup>. The Islamic Republic of Iran is suspected of having carried out cyber counterattacks in retaliation against U.S. banks, and successors to Stuxnet are still in circulation today. The extent of the threat posed by massive cyberattacks today and what *cyber diplomacy* is all about will be the subject of this report.

► Continue reading on page 20

## Social Bots – A Realistic Picture

A veritable bot hysteria has been observed in recent years, especially in media discourse. Automated accounts were ascribed a quasi-unlimited power in the manipulation of human discourse, especially in the field of politics. Myriads of intelligent program units imitate, almost indistinguishably, genuine human communication and generate entire new patterns of opinion. This simulation, an inauthentic discourse landscape, leads to more opposition to the free democratic basic order. This is the horror scenario that has been painted in newspapers, magazines and popular science publications for several years now.

However, this only reflects the real picture in a very limited and selective way. Let's take these two basic definitions:

- “bots, at their simplest, are social media accounts that are controlled either wholly or in part by software agents.”
- “[Bots]... are supposed to account pretending to be human users but which are operated automatically by malicious actors with the goal of manipulating public opinion.”

It is more, but also not less, in the case of so-called social bots. We can distinguish between three categories of these programs: non-automated, semi-automated and fully automated. It can be assumed that the majority of the observed accounts are semi-automated bots that, despite some autonomy, are nevertheless fully dependent on active control by a human user. This is followed by the non-automated bots, where a human user has to control all processes himself – this also includes large parts of the so-called fake accounts on the social platforms. However, this does not mean that every fake account is automatically a bot, because after all, the vast majority are created for purely personal purposes.

The actual number of completely automated bots, i.e. those that interact with people themselves and creatively, create and disseminate content themselves, with the cooperation of other, also fully automated bots, amounts to: approximately zero.

Of course, it is possible that secret technology already exists on this complex, or that new possibilities will open up in the future, through the use of AI. However, for reasons of scientific rigor, these assumptions cannot be addressed, as they are speculative, so all that remains is hard, empirical reality. There is no way to precisely identify a bot and even the supposed tools to do so have glaring methodological flaws, as Florian Gallwitz, Computer Scientist from TH Nuremberg also confirms.

His research mainly refers to the investigation of the reliability of the so-called botometer, a program created by Indiana University, which itself claims to be able to identify them on Twitter (now “X”) with high accuracy. The measurement categories of the Botometer are able to detect accounts with certain characteristics, but these say nothing about whether it is an automated process. The criteria on which this analysis method is based are not reliable enough.

For example:

The “Oxford Criterion”, which claims that posting 50 tweets a day increases the chances that a suspicious account is a bot

The Berkeley/Swansea approach claims that more than 10 – 15 tweets a day are reason to claim that an account might be automated.

These are interesting statistical features, but they do not prove that a suspicious account is really a bot or that a human is behind it. In actual use, the Botometer subsequently delivers quite curious results. In a 2019 test, for example, it identified 40% of the Twitter accounts of members of the Saarland state parliament as bots.

Even though the Botometer is more sophisticated, Gallwitz and Kreil explain why they consider it to be almost useless for the detection of social bots. First, they display the criteria under which the tool analyzes Twitter accounts, among them:

1. “Network features”, e.g. statistical features of retweet networks
2. “User features”, based on Twitter meta-data, such as account creation time

*“I have been researching the phenomenon for several years now and have to say that I have not been able to discover a single real social bot so far. In my opinion, this entire assumption is based on bad research.”*

Prof. Dr. Florian Gallwitz, Computer Scientist,  
Nuremberg Institute of Technology



3. “Friends features”, such as the median number of followers of an account’s social contacts
4. “Temporal features”, such as the tweet rate
5. “Content features”, based on natural language processing, especially part-of-speech tagging
6. “Sentiment features”, based on sentiment analysis algorithms (happiness, emotion, etc.)”

Further in their investigation, they examine the cases in which the tool misclassified Twitter accounts of true people as being social bots, and then they revisited the flaws in the categorization which led to these mistakes. As the authors claim, the hypothetical assumptions which created the framework for Botometer are too vague and blurry.

When Gallwitz and Kreil investigated the collected data sheets on selected accounts, they were not able to find a single example of a totally automated social bot that acts independent from human control, besides a lot of accounts that were not that “malicious” at all as they were presented in some papers.

It can therefore be stated that social bots, like many machines, are still completely dependent on control by humans and are also operated by them. This is not to downplay the actual danger of disinformation and false news. Nevertheless, the media nightmare

of automated, intelligent programs that independently and autonomously create and spread disinformation must be relegated to the realm of science fiction.

Gallwitz, Florian. Kreil, Michael (2022): *Investigating the Validity of Botometer-based Social Bot Studies*. Cornell University.



Research on Russian disinformation through Bots by the LMU Munich



**ARS TECHNICA:** Confirmed: US and Israel created Stuxnet, lost control of it. January 01, 2012.

By Nate Anderson.



### **The Mirai Botnet – cyberattacks against payment**

It is considered one of the most dangerous botnet systems that exists to date: Mirai. It is a malware that primarily infects computers that use Linux as their operating system. Thousands of computers are used undetected by Mirai to search for security vulnerabilities in devices that are part of the Internet of Things (IoT). Once such a one is found, the program plays itself onto these devices and initially remains undetected. At the command of one of the operators, only a few of which are known and convicted so far, the infected machines overload a target, such as a website, or a server, with thousands of requests until it collapses (DDoS – Distributed Denial of Service). Since its discovery in 2016, this network has been involved in numerous attacks on the websites of AirBnB, Netflix, Twitter, or even Rutgers University. The modus operandi: the perpetrators shut down a website with a DDoS and contact the owner, offering to seize the attack if a ransom is wired to them. Despite all the persecution, the Mirai botnet could not be deactivated and it is suspected that new operators, against payment of Bitcoins, continue to attack websites. What a DDoS attack is, how vulnerable the IoT is, and what can be done about it will keep us busy.

**Imperva:** Breaking Down Mirai: An IoT DDoS Botnet Analysis. October 26, 2016



## **Fancybear – a notorious hacking group**

It is beyond the scope of this article to list the numerous spectacular hacking attacks by Fancybear, a Russian group distributed among various units of the GRU military intelligence service. However, it is responsible for attacks on journalists critical of the Kremlin in Russia, the U.S. and Europe, on the French TV5 channel, the U.S. Democratic Party and the International Olympic Committee. In doing so, it uses a method it has perfected: so-called *spearfishing*<sup>5</sup>. In this process, the attackers imitate a real person who has information that can only be known confidentially between the sender and the recipient. However, as soon as the recipient clicks on a link contained in an email, for example, his or her computer can be infiltrated. This technique requires precise intelligence reconnaissance and a very targeted approach; you will read more about this in this report as well.



The world of hackers still fills us with fascination, but also with fear – because when using the Internet, there is always the fear of being hacked without knowing it. We are all aware that most attacks take place in the background and are successful if they go unnoticed.

### Sources and further readings:

**Amount of information circulating in the web:**

**Health-IT:** How big is the internet and how do we measure it.



**Internet of Things:**

**McKinsey:** What is the Internet of Things?  
August 17, 2022



**Botnets:**

**European Union Agency for Cybersecurity (ENISA):**  
Botnets



**Crowdstrike:** WHAT IS A BOTNET?

January 12, 2022



**Shadowserver** collects vast amounts of threat data, send tens of thousands of free daily remediation reports, and cultivate strong reciprocal relationships with network providers, national governments and law enforcement.



**Deep Fake**

**Bundesregierung:** Deepfakes: Ist das echt?  
(in German) June 28, 2022.



```
(n, _) {  
    t.Event("keyup");  
    n.trigger(o)
```

```
    .extend({  
        length: 0,  
        element: t(""),  
        selector: "#ub-ac-outer",  
        "#ub-ac-inner",  
        "id=|ub-ac-out",  
        container: !0,  
        mode: !0,  
        arch_all_button: !0
```

The Programming code is the basis of cyberspace, which is another reason why many people are uneasy about this technology. We all use it, but hardly anyone really knows how it works. Nevertheless, you don't necessarily have to be a programmer to get to grips with the subject – that's what this chapter is all about.

# 3 Introduction to online disinformation and cyber insecurities taxonomy and terminology

---

The subject areas of online disinformation and cyber insecurities are full of technical terms that are difficult to understand to non-tech audiences. To complicate matters, such technical terms are often so-called neologisms, i.e. newly created words. These often originate from the so-called **net culture**, i.e. social groups such as software engineers, but also passionate computer gamers and people who frequent forums and discussion platforms. They are also words from everyday life that are used for their symbolism to describe phenomena on the Internet. We stick to our proven distinction between online disinformation and cyber security, otherwise, the clarity would be lost.

## Taxonomy

### Cybercrime

When the term “hacking” is mentioned, people immediately think of cybercrime, but as we will explain, this is too narrow. Even the term cybercrime itself is not as clear-cut as one would initially assume. In the German-speaking world, a distinction is made between crimes that occur on the basis of the Internet and those that use the Internet only as a means. This sounds very abstract, but in the narrower sense it means that cybercrime uses the computer as a weapon to obtain goods without permission. The crime does not have to

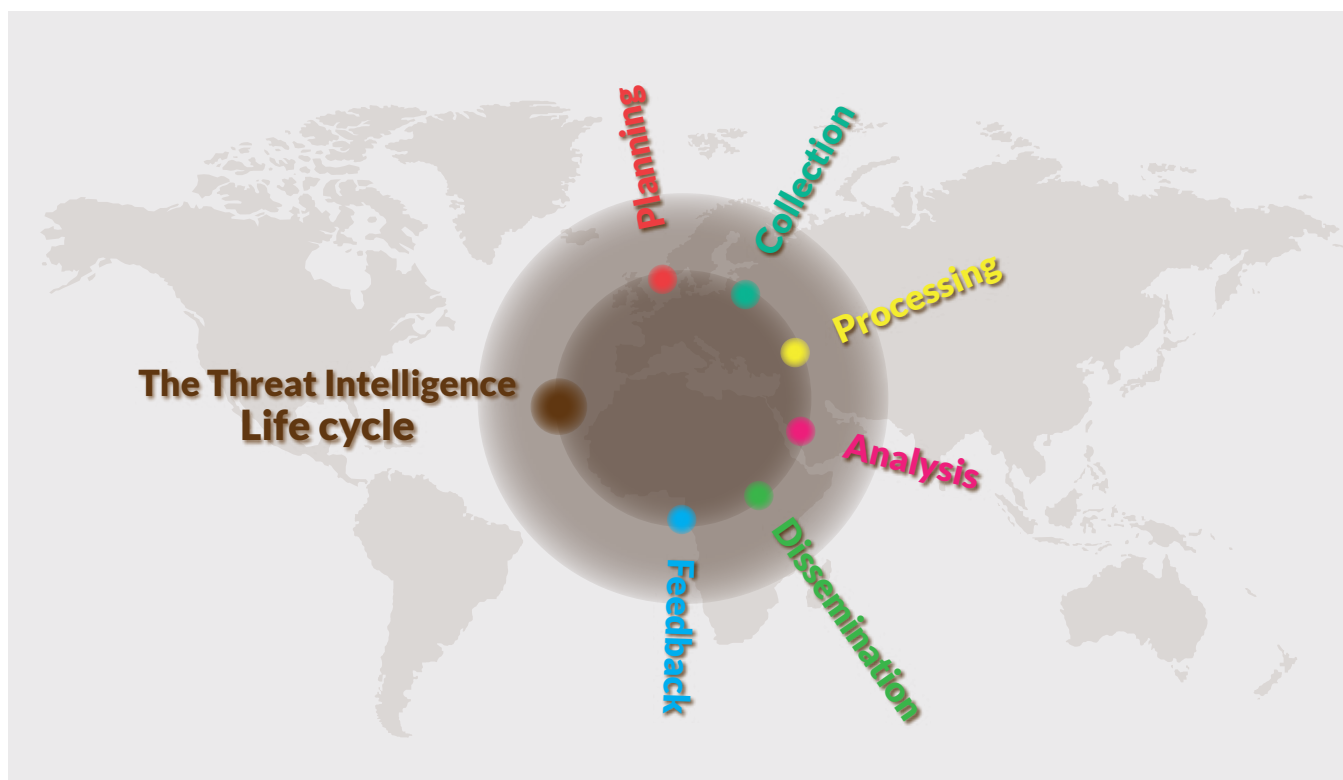


Figure 3: Coordination and logistics of cyber attacks. Courtesy of cybersecurityforme.com

be possible without a computer. US criminal law recognizes the criminal offense of wire fraud for this purpose. Cybercrime in the broader sense, in which the Internet is used as a tool, includes crimes that would otherwise be possible without this technology. This includes, for example, defamation, blackmail and coercion. Of course, other phenomena of cyberspace can also have aspects of cybercrime. For example, so-called “patriotic hackers” such as those used by Russia may well engage in money laundering, or use blackmail to disguise their origins, for example, or even recruit members under duress. Despite all this, it is not organized cybercrime. The distinguishing criteria are important here.

### Cyber Espionage

Cyber espionage encompasses the entire effort of intelligence agencies to obtain information on the Internet through means of infiltration that are not publicly available. However, likewise the placing of compromises, or the unauthorized interception of telephone calls via the Internet and techniques for concealing one’s own activities.

In addition to political cyber espionage, there is also economic cyber espionage, which uses the same methods, but again generally speaking, has different objectives. Of course, mixed forms are also possible here. For example, the People’s Republic of China actively spies on foreign research institutions through state institutions in order to give its own companies a competitive advantage.

By its very nature, cyber espionage is never an end in itself, but a means and a basis for further activities by governments and their intelligence services. It can be carried out directly by government bodies, but also by hacking-for-hire and so-called “patriotic hackers” to cover tracks. Cyber espionage serves to:

- Gain intelligence for governments and are thus of strategic relevance in foreign policy.
- spying on vulnerabilities and access points
- Compensation of backlogs in research
- Identifying captious points on groups and individuals, and developing and placing a compromise.



## Cybersabotage

Cybersabotage uses acquired knowledge and access from cyber espionage to cause targeted damage to foreign systems. Either political groups, other states or companies can be attacked. The range of actions is extensive and is discussed in more detail in the terminology on cybersecurity, as well as in the points on

individual scenarios and states. An important question when discussing cybersabotage is how it differs from cyberwar and whether there is such a thing at all. More on this in the Infobox.

In order to be able to precisely delimit the term here, we define cybersabotage as attacks on non-critical infrastructure in

► Continue reading on page 28

### The distribution of cyber attacks across CSEP dimensions.

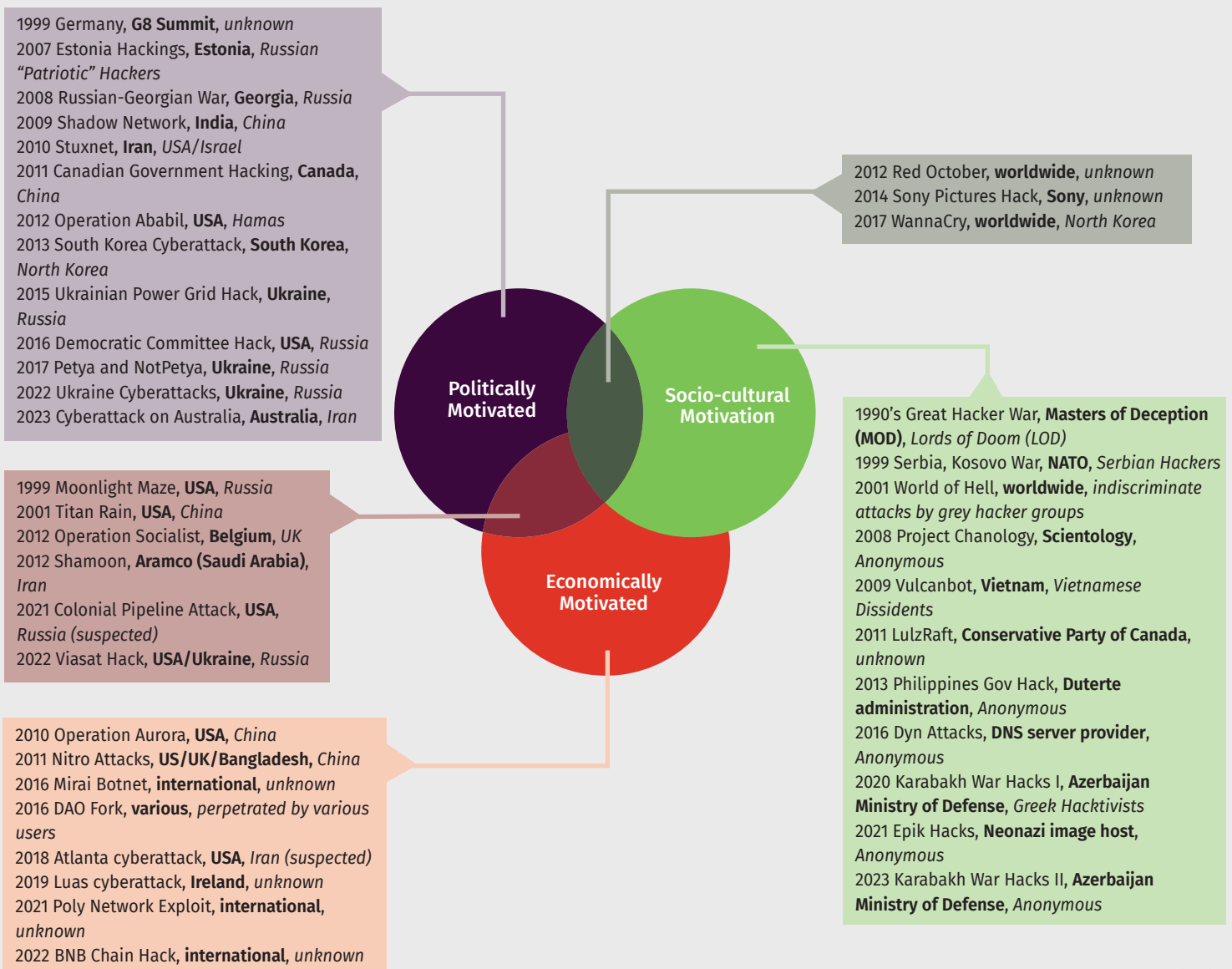


Figure 4: It depends on the motivation what characterizes a cyberattack. Source: IEEE Technology and Society Magazine.

## Cyberwar, cybersabotage and the difficulty of attribution

In order to be able to react adequately to threats from cyberspace, it is an absolute prerequisite to be able to reliably determine and trace the perpetrators. However, this is where the first problems arise, because in practice this is more difficult than it may sound.

The EU does not have an efficient method for attribution within a reasonable period of time. However, time is of the essence when it comes to successfully implementing countermeasures.

The first distinction between cyber sabotage and cyber war already begins in the detection of traces indicating authorship. While sabotage is clandestine and tries to avoid any conclusions about the perpetrator(s), cyberwar is a deliberately belligerent act by a nation that also wants to make sure that an action is understood as its own.

Although this distinction provides some clarity between the terms, in reality it makes it even harder to determine exactly who is now responsible for an attack. Of course, certain groups, or even state

*“Attribution” is a short word and sounds so simple. From a software engineer’s point of view, however, it is very difficult to ensure rock-solid proof of the actual authorship of an attack. The ‘smoking gun’ does not exist and it remains a hunt for circumstantial evidence.”*

Mustafa Isik, Software Engineer and IT scientist

Different levels of Cyber Attacks and Responses				
Aim	Prevent (peace)	Discourage (peace)	Deter (hybrid)	Respond (war)
Dynamic	Resilience	Investigative	Active Defense	Retaliation
Threat Dimension	Backdoors, Zeroday Exploits	Cyber Crime, Black Hat Hacking, Trojans	Data theft, Extortion, Data Corruption	Attack on Critical Infrastructure
Remedy	Certification	Threat Hunting	Counterattacks on Source	Counterattacks on Critical Infrastructure
Institution	Joint Cyber Unit, ENISA, CERT-EU	Europol EC3	ENISA, EU INTCEN, EUMS INTEL	Cyber Defense Force (Cyber-Rapid-Response Team CRT), NATO
Challenges	Unkown post-production flaws	Borderless hybrid threats	Attribution	Escalation

Figure 5: Various challenges and various courses of action depending on the threat in cyberspace. Source: Inhouse.

*“The political intention is to be deliberately unclear about what constitutes an act of war in cyberspace and what does not. The intention is to keep the adversary in the dark so that it is not encouraged to test a defined threshold that could trigger a counter-reaction.”*

Dr. Annegret Bendiek, German Institute for International and Security Affairs (SWP),  
Deputy Research Group Leader  
Cybersecurity and Digital Policy



actors, also use their own specific programs and have their own specific approaches to attacks. This allows for some inference, but is the “evidence” authentic? During various hacker attacks, code was apparently discovered that contained Chinese characters (see -> Cyber strategy of the People’s Republic of China), which quickly led to the conclusion that Beijing was responsible for various acts of cyber sabotage in Western countries. The only problem here is: This kind of “evidence” may have been deliberately placed by the attacker to distract attention from himself. It is easy to do this and the opposite cannot be proven, all that remains is the diplomats’ assurance of no responsibility and so, despite everything, it is still testimony against testimony.

The situation is somewhat different in the case of cyberwar. In theory, no special investigation needs to be done here; the executing state wants the attack to be perceived as its own. In the sense of war as a continuation of diplomacy by other means, following Clausewitz, it is desired by the attacker to be seen as the responsible party.

But here, too, various problems arise. Does cyberwar even exist? Various difficulties arise when the phenomenon is examined in detail. Such a conflict,

which began on the online level and also had its main venue here, has not yet taken place on a larger scale. It is therefore a speculation about a phenomenon that has not yet taken place.

To be sure, there have been attacks, such as the attacks on the KA-SAT network (also known as the VIASAT attack) in the run-up to the Russian forces’ invasion of Ukraine, or in 2015, when the power grid was paralyzed in western Ukraine. However, there has not yet been an attack designed to affect the entire viability of a country.

The renowned RAND Institute warns against a settling perception of potential cyberwar in Cold War categories, more specifically, those of nuclear deterrence. Cyberattacks are not weapons of mass destruction and should not be perceived as such. They therefore recommend using the term “Weapons of Mass Disruption” because, in their analysis, the potential of cyberattacks would be to weaken and create chaos rather than to destroy the adversary.

This is because military doctrine is clear: the application of a WMD can only be retaliated against by equal means.



Figure 6: Different kind of information, from trustful to distrustful, from constructive intend to harmful intend. Courtesy of eavi.

which no persons are harmed. Seen in this light, the Stuxnet attack on the uranium enrichment facilities in Bushehr, Iran, was an act of sabotage and not an act of war.

The goal of cyber sabotage is to disrupt routines at an adversary and thus stop, slow down, or make processes impossible. The extent to which companies also use this practice among themselves is unknown. However, companies have already been the target of such attacks, but again the line between cybercrime and cybersabotage can be blurred. Again, it depends on who is responsible.

### Cyberwar

In this compendium, cyberwar will be defined as any attack by computer-based means on a country's critical infrastructure. The goal is to damage, destroy, or render unavailable indefinitely the vital functions of a state.

This includes electricity supply, gas and fuel supply, water supply, transportation security, telecommunications and data security, finance, and emergency services. Here again, cyber espionage intelligence is exploited to find vulnerabilities in the shielding and

security of these systems to enable infiltration. Subsequently, either so-called -> logical bombs are introduced, or so-called -> zeroday exploits are spied out. These means are always a means of ultima ratio, after which no further diplomatic solution is sought, but the “solution” of open geopolitical questions with warlike means. This is also the reason why it can be assumed that a cyber attack will always be followed by conventional attacks. Despite all this, the concept of cyberwar is controversial, more on this in the Infobox.

## Terminology of Online Disinformation

Online disinformation mostly takes place on so-called **social networks**, which are platforms on the Internet where people network with other people, communicate with each other and also inform themselves. These include Facebook, Twitter, Instagram, Snapchat and Telegram. In the latter case, this is also an instant **messaging app**, often called a **messenger**. In short, this is a program where you can exchange quick short messages via your own phone number – but you can’t create your own multi-layered profile, as you can on Facebook, for example.

**Profiles** are virtually every user’s own little website, regardless of the service. These personalized pages are usually populated with the user’s own pictures, information about birthplace, education, hobbies, and much more. But don’t be fooled by this, because although the majority of these pages look authentic, the people portrayed are in some cases when we enter the field of online disinformation not real. They are so-called fakes, which only imitate a really existing person on the net. The magnitude of this is difficult to assess, but we can estimate that on Facebook alone there are 1.3 billion fake accounts as in the fourth quarter of 2022. If these fake profiles are equipped with professionally manipulated images or video clips in which the person portrayed is also non-existent in real life, this is known as a **deepfake**. These deceptive imitations of apparently real events even include fake videos of world political events, as we also mentioned at the beginning in the case of the “Ghost of Kiev”. There, air battles can be shown that never took place, politicians can be shown making speeches they never gave, and technical achievements can be praised that do not exist.

News can also be faked, they describe events that have never taken place in this way or in the form described, they relate events that are strongly distorted or have been completely confabulated. In this case, we are dealing with **fake news**.

Fake profiles are used by an individual, a group or a program to spread such “news”. If several such fake profiles are used simultaneously, this is referred to as a **bot network**. This can be **automated**, i.e. controlled by a program, **semi-automated**, by a program with direct support by a human, or **non-automated**, fully operated by a real user. Semi-automated bot networks are the most common form.

These networks are used for the mass dissemination of messages and content, they try to suggest that there is a real debate. **Simulated discourse** is what this is called, because the “participants in the conversation” don’t actually exist, they are various fake profiles, controlled by bots, sometimes more, sometimes less automated, but usually always involving real humans that coordinate them – and people with real political interest organizing the technical and material infrastructures necessary to maintain such networks.

However, another technique is also used, if the aim is to prevent a topic from being visible in the first place, or to hinder a discussion on social media, it is called **message polluting**. Even nonsensical messages, replicated and spread thousands of times, can already bring a serious discussion on a topic to a standstill. Imagine you are in a bar with a few friends talking about a trip, and suddenly a hundred people come and start shouting at you from all sides. Wherever you go, the mob goes along with you until you are unnerved and cancel the meeting. That’s exactly what message polluting is.

Like all social groups, any grassroots movement thrives on the number of individuals committed to it. But what do you do if you have only a small, or even no members in an online movement? One operates so-called **astro-turfing**. By faking personal profiles, you give your own group, on Facebook for example, thousands of members, all of whom exist only on paper – or in this case in bits and bytes. However, this does not make a difference, because for untrained eyes it is not obvious and it is assumed that a certain movement would apparently experience enormous approval. This popularity and the spread of a certain message is also called range, i.e. how often something was read and how often it also comes to an **interaction**. This means that people engage with

a message, for example by commenting on it or sharing it on their own site, i.e. **reproducing** it. This is exactly what online disinformation aims at.

How does Online Disinformation work? Read this non classified paper that was awarded a NATO Early Career Researcher Award in 2022, written by Anna Reuss and Lucas Maximilian Schubert (Chair International Politics and Conflict Studies, University of the Bundeswehr Munich).

**How does Online Disinformation work? Read this non classified paper that was awarded a NATO Early Career Researcher Award in 2022, written by Anna Reuss and Lucas Maximilian Schubert (Chair International Politics and Conflict Studies, University of the Bundeswehr Munich).**



*“Hacking is an exploitation of some system that subverts the rules or norms of that system. This often hurts the system but is not always something that is explicitly forbidden; much hacking is simply something not anticipated or intended by system designers. Of course, when we think about hacking in the modern context, it is hard not to think of computer or other networked devices. But hacking is an activity that can be generalized to human systems broadly. Systems of economic activity, systems of government, systems of democratic or other governance, systems of social behavior – these are all hackable constructs.”*

Christopher Whyte, Expert

## Terminology of Cyber Security

The Internet is no longer the curiosity and ultimate technological innovation it was in its early days. In 1990, when the decision was made to release the ARPANET, which had been used for military and scientific purposes, for civilian use, the Internet was born.

What was accessible to very few people at the time and had virtually no influence on the real, physical world, is now directly interwoven with almost all aspects of it. This ever closer interconnection is also known as the **Internet of Things (IoT)**. Everyday objects, as well as machines and administrations, exist outside but also inside cyberspace. They contain chips, and small computers with operating systems, through which their functions can also be controlled remotely, via the Internet.

Imagine that you buy a washing machine from the higher price segment. Just twenty years ago, the machine would have done only what it did all those years before: Wash clothes at the push of a button. Of

course, there was also technological progress, more functions, more electronics. Still, you couldn't turn your washing machine on and off while sitting a thousand miles away. Today, however, that is possible because your appliance is what is now called “smart”: it has access to the Internet and can be controlled remotely. You can monitor the washing process, adjust the temperature and much more, through an **app**. This is the abbreviation for **Application**, which is a small program that allows you to perform certain specific operations. Like, for example, the control of your washing machine.

But not only the washing machine or your stereo sound system that are connected to the network, but also, for example, the production lines in the automotive industry, the databases and the administration of your health insurance company, the turbines and generators of the electricity company and, more recently, the electricity meters. This facilitates their maintenance and precise control, but it also makes them vulnerable



Figure 7: 11 Hacking Statistics. Courtesy of cybersecurityforme.com. Iconcredits see page 131.

to malicious manipulation and increases the possible range of errors.

Each individual device has an **IP address** which makes the device exactly identifiable on the Internet. This circumstance can be exploited by **hackers**, i.e. people with sufficient IT knowledge who specialize in penetrating computer systems in order to manipulate, investigate, examine or even destroy them. Hackers are often associated with malign behaviors, however this notion is outdated. While **black hats**, like their Wild West cowboy counterparts, actually seek to do harm, **white hats** seek to identify security vulnerabilities and work with website operators to fix them. **Ethical hacking** falls into a gray area, where attempts are made, for example, to penetrate the systems of dictatorships, malicious cults and corporations that are perceived as corrupt. It is not always clear whether the groups are acting autonomously, as a civil initiative, or whether they are in fact state actors. So-called **attribution**, i.e., the precise attribution of a cyberattack to a perpetrator, is not yet mature enough to be able to say with certainty who exactly is behind such an action.

The **rootkits**, specialized programs that can remotely control devices without permission, are also available for purchase on the dark web and can, with some prac-

tice, also be used by private individuals without great expertise. The **dark web** must be distinguished from the **deep web** and the **surface web**. In the latter case, it is the conventional Internet, as we all use it every day: you open the browser of your choice and use a search engine. You have also most likely downloaded this report as a PDF file from a page on the surface web. The deep web is all the databases, such as government archives, health insurance data, and non-public corporate documents, that they cannot access with their browser and are unlikely to be found by any search engine.

The dark web is a structure that exists on the Internet via so-called **peer-to-peer networks**. Only partial information on the respective websites is stored on many different servers, and large computers that serve as nodes, and it is not possible to use a search engine to find them. Therefore, you need the exact dark net address of a website and you also need to have a special browser, **TOR (The Onion Routing)** to reach it. There are several archives of dark web addresses on the surface web, through which individual pages can be accessed. It stands for all kinds of illegal activities: Drug trafficking, human trafficking, trafficking in weapons of war, child pornography and also software piracy. However, the dark web also opens up the possi-

## 10 Biggest Ransomware Attacks of 2021

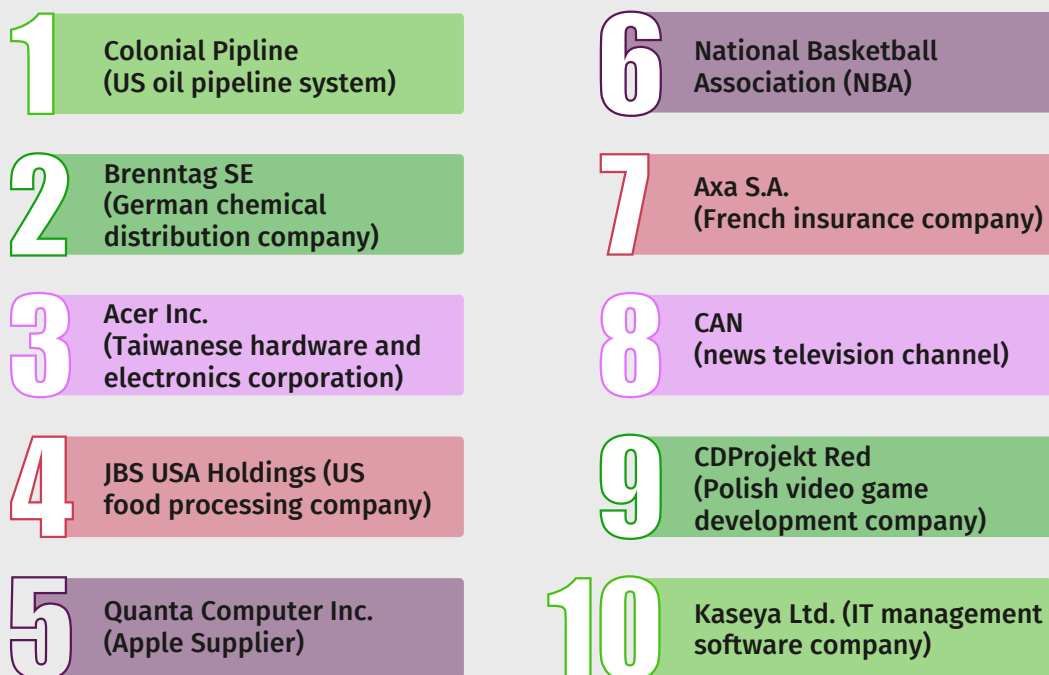


Figure 8: Biggest ransomware attacks in 2021. Courtesy of cybersecurityforme.com – Touro College

bility for dissident groups in totalitarian states to communicate securely and untraceable.

Hacker groups also frequently offer their clandestine services on the dark web. However, **codes**, i.e. source data, can also be downloaded for the construction of own malicious programs, called **malware**. This includes various **computer viruses**, specialized programs that penetrate systems and manipulate their functionality, or even hinder and destroy them. They have various subcategories. **Ransomware** prevents you from accessing certain data, often offering to unlock it for a fee. **Trojan horses** first try to disguise themselves as useful, normal programs and then unleash their destructive effects. A **worm** represents only a small fragment of a malicious code that infects “healthy” files on your computer and causes them to change its behavior.

**Passwords** are essential for computer security, but they are by no means indispensable. **Spyware**, once on your computer, spies on your security data and sends it

to the sender of the program. Undetected, a small portion of your computing power can be used to turn your computer into a so-called **bot**, a device that performs actions remotely, covertly and autonomously over the Internet. Many such infected computers connected together form a **botnet** that can be used for so-called **DDoS attacks**. **Distributed Denial of Service attacks** are in principle quite simple: a botnet sends thousands of requests to a website until it collapses and can no longer be reached. What sounds like a prank at first, however, has proven a great challenge for commercial and administrative sites in the past, which were sometimes unreachable for days.

To defend against viruses, attacks and spying, a number of protective measures exist. **Antivirus programs** are provided by web forensics companies, which are constantly updated and can detect and remove harmful programs. **Firewalls** protect computers from unauthorized remote access and control incoming data, for example from **data theft**. This is the case, when hack-



## TAXONOMY & TERMINOLOGY

ers try to steal sensitive information from devices, especially during cyber espionage. Not only private, but also commercial computers and servers require protection and, in addition to antivirus programs and firewalls, often have trained support personnel who take care of them professionally and on an ongoing basis. Above all, **critical infrastructure** facilities – all those areas that are important for the functioning of modern society. In Germany this is legally defined as energy and water supply, food, telecommunications, medical care, finance and insurance, as well as transport and aviation.

They are now inextricably linked to the Internet and can no longer be disconnected from it without becoming dysfunctional. The Internet has become one of the

lifelines of our modern civilization. That's why cyber protection is also a vital component of a functioning society.



Malware often nests undetected on computers and often even pretends to be useful software.



Phishing is very often the “foot in the door”, which is then followed by the bigger attack.



Firewalls are often portrayed as impenetrable barriers. However, this is not true.



How are international players taking action to bring some order to the chaos of the web? What appears on the surface to be a classic policy problem is actually much more complex and difficult than anything that has gone before.

### 4

# Online disinformation & cyber insecurities: international frameworks and regulations

---

It is a natural human endeavor to bring things into some form of rules and order – because a lack of rules leads to uncertainty and poor plannability, which in turn also leads to threatening situations for society, the state and the economy.

For exactly the same reason that traffic signs and traffic lights exist, attempts are also being made to establish traffic rules for the Internet. This chapter will not initially go into detail about the gaps, problems and deficits in international regulations and institutions. Instead, it is intended to provide an overview of the nature of the regulations and the institutions that attempt to enforce them and monitor compliance with them.

National and supranational legislation as well as international law attempt to exert a normative influence on the use of and access to the Internet. This expression has two dimensions for the Internet phenomenon, one social and one legal.

Social norms are very simplified rules that ideally everyone in a given group adheres to at all times and that are, mostly, unwritten. Legal norms are always written down and attempt to ensure compliance by means of sanctions, the exercise of which is, in the case of the EU, in the hands of national and supranational institutions.

So who sets rules on the Internet and who “watches over” them? Well, that is not so easy to answer. Imagine

playing a board game with your family or friends. This game is about information, trade, but also influence. The board and the squares are visible to everyone, they all use the same square and everyone occupies a certain area on it with his pieces. There you decide what is valid, as each player on his field, but on the whole there are no exact rules. You have to negotiate them first, but while goods continue to be exchanged and event cards are drawn, which have an influence on you and your fellow players.

Replace the game board with the Internet, yourself and your fellow players with states, and the characters on their territory with institutions, and you’re very close to the picture of how things work in cyberspace.

States have their own legislations that are supposed to regulate behavior on the Internet. National regulations lose their effect if undesirable events happen abroad. This is exactly the problem we find in cyberspace. For this reason, the UN, for example, but also the EU and its member states, are trying to achieve a certain degree of standardization.

Legal norms and institutions go hand in hand with treaties, because neither would exist if they were not preceded by multilaterally negotiated documents. That is why it is important to look at which treaties already exist and which recently concluded ones will be relevant in the future:

**Budapest Convention on Cybercrime (2004)**

Copyright infringement, wire fraud, child pornography, violation of network security



**Additional Protocol to the Convention on Cybercrime (2006)**

Inclusion of racism and hate speech in the convention



**Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (2022 – open for ratification)**



**United Nations Convention on the Use of Electronic Communications in International Contracts (2005)**

Use of digital communication in international trade



**The United Nations, the International Telecommunication Union, and other international organizations**

One of the first conferences that arguably set the tone for the rest of the process was the World Summit on the Information Society (WSIS) held in 2003 by the United Nations and the International Telecommunication Union. For the first time, multilateral negotiations were held on the areas of cyberspace in which multilateral solutions must be sought.

Points were identified there that continue to concern us today.



- Reducing the “digital divide” between the Global North and the Global South
- Digitalization of Public Administration
- Equal and immediate access to information and knowledge
- Security of the Information Network

**World Summit on the Information Society (WSIS) in 2003**



The International Telecommunication Union (ITU) in Geneva is the affiliated organization at the United Nations that tries to reach standardized procedures, conventions and agreements on a multilateral level. However, this is very difficult because, as in the main plenary and the Security Council, states with very different interests and agendas are members.

It is divided into the main plenary, the permanent conference of all 193 member states in the ITU. It is the decision-making body and meets every four years.



WSIS (World Summit on the Information Society) was a pioneer in establishing an international negotiation format for the Internet, communication and digitalization. The format, initiated and supported by the United Nations and the ITU, brought together international players on this topic for the first time at a special summit in 2003.

There, the general working guidelines, topics and areas of activity are determined, and resolutions and decisions are passed by all member countries. In addition, there is also the Council, divided into five world regions, staffed by selected members. It serves as a policy body for the implementation of the resolutions. The Secretariat deals with administrative tasks and services.

Below it are the so-called sections, which deal with special issues and whose results are transmitted directly to the main plenum. These include ITU-R (Radio telecommunication), ITU-T (Standardization) and ITU-D (Development).

The ITU-T, the most important section, has standardized various technical aspects of the Internet that we use every day, even if we may not be aware of it. Among them, for example:

- X.509: Certification formats for encryption systems in Internet communication
- Trustworthy AI: Standardization of secure, artificial intelligence to protect online privacy
- X.805: Security architecture for systems providing end-to-end communications
- Coding of still images: JPEG picture format

## International Telecommunication Union



If you have ever wondered how exactly the individual address endings on the Internet come about, the answer to this is: there's an organization that deals with this, too. The Internet Corporation for Assigned Names and Numbers, ICANN for short, manages the allocation of the so-called top domains. These are the abbreviations that you will also be familiar with such as .net, .org, .com and many more.

In addition, the IP addresses, with which a computer is exactly identifiable in the network, are assigned on the basis of five world region blocks, the computer time zone databases are managed and the network protocols are defined, which make it possible for computers to communicate with each other on the Internet.

**ICANN** was not founded as a company by a multilateral agreement, but was given this function by the former operator of the Arpanet, the military-scientific precu-

sor of the Internet, named Defense Advanced Research Projects Agency (DARPA). The main criticism of ICANN is that most of the root servers, i.e. where the name registers are stored, are not decentralized but located in the USA and that no official supervisory body has been watching over the company's activities since 2016<sup>6</sup>. It was considered to have this determined by the UN, but there is still no decision to this effect.

**ICANN**



But international organizations are also active in the field of law enforcement assistance. INTERPOL, one of the oldest institutions established by multilateral agreement, and which has also operated close to the UN as a non-governmental organization since 1949, maintains various subdivisions and projects that deal specifically with the prevention, mitigation, and prosecution of cybercrime.

INTERPOL's Cyber Fusion Centre gathers experts from member state law enforcement agencies, as well as from big tech companies, and aims to provide early warnings about existing, evolving and potential new cyber threats. The center also sees itself as a place for stakeholders to share intelligence, and since 2017, it says it has already produced 800 reports on ever-changing threats, such as phishing, hacked government sites and malware.

**INTERPOL**



## The European Union

The EU as a supranational political system and political community yields considerable power and relevance when it comes to regulating and combatting online disinformation and cyber insecurities. In addition to the EU level, the individual member states all have quite different legislations that are valid on their territory. The goal of the EU is to harmonize these regulations and establish common standards, but also to offer very concrete solutions and work in real time to provide critical information to member countries by establishing EU-wide regulatory frameworks and responses.

For this purpose, various institutions exist on the territory of the European Union:

- Interpol EC3 (Administrative assistance for the prosecution of cybercrime)
- ENISA (Hazard identification, consulting and development of solutions for EU countries)
- EUINTCEN (Intelligence sharing, satellite reconnaissance)

Around the same time that the WSIS began its work, the European Union also began to set up an organization to deal with security in cyberspace: ENISA.

The European Network and Information Security Agency, based in Athens, aims to provide advisory support to individual member states and to help improve the cybersecurity of the entire Union through solutions it has developed itself. It also participates in the process of aligning the various national regulations to an EU standard.

To this end, ENISA has defined six areas of responsibility:

- Development and implementation of Union policy and legislation.
- Capacity building for prevention and mitigation
- Operational cooperation at the Union level
- Knowledge and information
- Awareness raising and training
- Research and innovation

ENISA proved capable of adapting its own agenda and expertise to the changing and highly volatile situation in cyberspace. In 2019, ENISA was transformed from an organization whose mandate had to be renewed annually into a permanent form. In doing so, the European

Union underscores the importance it attaches to countering threats from cyberspace to the community.

Although the structure has remained unchanged with the management, as well as the executive board, since 2019 the individual member states of the EU are also directly represented at ENISA with a permanent liaison officer. Likewise, so-called “stakeholders” (companies, research groups, consumer protection associations, etc.) are directly connected to the agency. This means that work can be coordinated more quickly and efficiently.

### ENISA works closely with, among others:

- Bundesamt für Sicherheit in der Informationstechnik (Bonn, Germany)
- Agence nationale de la sécurité des systèmes d’information (Paris, France)
- Agenzia per la cybersicurezza nazionale (Rome, Italy)

Solutions to cybersecurity problems are constantly being re-engineered to stay “on the ball” in the ever-changing Internet. Some examples:

- Good practices for the security of healthcare services (during the Coronavirus Pandemic)
- On-line tool for the security of personal data processing (2020)
- National Cybersecurity Assessment Framework (NCAF) Tool (2022)

However, it is not only within the Union that the EU seeks to strengthen cooperation and collaboration, but also with so-called “third countries”, i.e. countries that are not members or are even outside Europe.

EUINTCEN (EU Intelligence Analysis Centre) works as an institution of the European Union on the networking and exchange of intelligence of the individual intelligence services of the member countries, as well as on the cooperation with security services of third countries.

What is special about EUINTCEN is that the center, founded in 2003, existed in a legal gray area, as it was not covered by any EU law. This ambiguity lasted until the Lisbon Treaty in 2007, through which the institution was subsequently legitimized.

EUINTCEN is neither accountable to the EU Parliament nor to the national parliaments and does not allow them to see its documents. Only the European Commission and the individual national intelligence services are authorized to receive information from the center. EUINTCEN does not conduct any active intelligence activities itself, but bases its findings only on information voluntarily provided by its individual members. This cooperation is relatively slow, since the German BND, for example, only forwards documents with the lowest classification level to EUINTCEN. This leads to a situation where the center’s work has repeatedly been described as deficient.

### Read the Statewatch report 2013 on EUINTCEN



In the field of cybercrime prosecution, EUROPOL, the EU’s overarching police mutual assistance organization, launched “EC3” in 2013. As with INTERPOL, EUROPOL is not directly a law enforcement agency with state powers. Therefore, EC3 is also an advisory body for the exchange of information and the improvement of the work of national police forces in the area of online crime.

The EC3 has three working groups:

- Crime with a connection to cyberspace
- Fight against child pornography
- Payment fraud (Wire Fraud)

In addition to the individual member states of the European Union, the EC3, as well as the entire EUROPOL structure, cooperates closely with non-member states and organizations. For example, with the INTERPOL, the United Nations, the USA, the European non-EU members, Canada and Australia.

As was mentioned at the outset, the Internet is already directly and immediately connected to our physical everyday life through the Internet of Things. However, there is also another level that could confidently be called the Internet of Social Fabric as well. If we look closely, we will see that large parts of our social lives already depend on the digital world. We tweet, text with friends on Facebook, post pictures on Instagram, apply for jobs on LinkedIn, listen to music on Spotify, shop on Amazon, do our tax returns online, some have

even met their life partner over the Internet – this list could go on and on. According to the 2023 figures by the online shipment company Oberlo, the number of digital buyers is at 2.64 billion, which makes up 33.3% of the population worldwide<sup>7</sup>.

Issues such as privacy, commerce, confidential information, but also news, intellectual property and communication are regulated by laws that were preceded by a political decision-making process in parliaments.

At this point, we will introduce an important concept that is important for understanding cybersecurity, but also how the issues of politics, cyberspace, security, and civil liberties are important: the so-called “**securitization**”.

**Read the IMF definition and analysis on Securitization**



This term first refers, in simplified terms, to the fact that various fields of public life and society are put on a “security agenda” in order to be able to defend against threats with which political institutions are faced. These include, for example, fields that are not otherwise directly cognitively associated with a security issue. Private communication, copyright, freedom of movement, or even data traffic on the Internet.

However, this also means that security institutions have a tendency to view all areas of life from a security perspective and to generally view them as a potential security problem. The consequence of this can be that civil liberties are problematized and a threat that civil liberties are curtailed becomes a clear danger.

A contemporary phenomenon relevant to our focus topic, cybersecurity, is the so-called data retention, which is still causing controversy today and serves as one of the prime examples of the intertwining of the topics of politics and privacy through cyberspace. After the manifold serious terrorist attacks between 2001 and 2015, the problem was seen in the open communication that enabled the perpetrators to exchange information and obtain instructions over many thousands of kilometers in order to plan an attack.



Personal data security is a top priority these days. However, it mistake is always using the same passwords, even for very carelessness is responsible for most security breaches





is often not the systems that fail, but the human factor. A classic sensitive platforms such as online banking. This kind of on the Internet.

After 9/11, demands were made by interior ministries of some Western countries, but also by the European Union itself, that telecommunications should be monitored, even without specific grounds for suspicion. A letter from then U.S. President George W. Bush to Commission President Romano Prodi in October 2001 expressed the demand that all regulations requiring the regular deletion of telecommunications data to ensure privacy be repealed<sup>8</sup>. It further demanded that the EU be able to secure this data for a “reasonable period of time.”

However, it was to take some time before the EU could agree on so-called data retention. Directive 2006/24/EC allowed accurate data on telecommunications connections of all EU citizens to take place for a minimum period of 12 months and a maximum period of 36 months. Under the impact of the terrorist attacks in London in 2005, the EU Parliament and the Council of Ministers finally voted in favor of the directive. Although the scope of the data to be stored was somewhat reduced by the parliamentary debate, the list nevertheless remained glaring:

- All dialed numbers of all mobile subscribers
- Time of the calls
- Duration of stay on the Internet for each IP address, as well as about the type of service used
- Names and addresses of all IP addresses and phone numbers

What initially even sounds very modest from today’s perspective had extensive effects that are still noticeable today. Directive 2006/24/EC was implemented in various forms in the national legislation of the member states.

Although the directive was declared invalid by the European Court of Justice in 2014 because it is not in line with the EU Charter of Human Rights, individual member states have already established their own regulations, legislation and informal patterns of state action (for example Data Retention and Investigatory Powers Act, DRIPA in the United Kingdom).

**Read the Jonesday legal analysis on Directive 2006/24/EC**



It is literally like the metaphorical breach of the dam, or Pandora’s box: once a political step has been taken in the field of cyberspace, it is difficult to control its implications or to reverse the entire step. In other words: once a securitization of a certain question has begun, it is quite hard to stop it.

In Germany, too, the Federal Constitutional Court established back in 2010 that the national laws created under the impression of the directive were incompatible with the Basic Law. Nevertheless, one should not be under the impression that this has finally put an end to data retention and surveillance on the Internet.

In new attempts at legislative initiatives, attempts have been made to reintroduce it, but were refuted in the Federal Constitutional Court in 2023<sup>9</sup>. Yet in other member states of the European Union it still exists – and also in the United States, where it originated and has also been extensively expanded, refined and consolidated.

The argumentation has extended to several areas on the Internet, which, from this point of view, no longer have anything to do with counter-terrorism. Lobbyists of a strong protection of copyrights argue, for example, that without a storage of IP addresses of every citizen, no anti-abuse protection in the area of protected trademarks, names, products and patents could be guaranteed. So, as we can see, the “securitization” of communication on the Internet, of individuals, groups, companies and all other social associations of people, is very advanced and probably irreversible. Is it running out of control?

However, the classic storage of IP addresses and their activity patterns, i.e., to put it bluntly, of identifiable individuals and their browsing behavior, has given way to more sophisticated monitoring options in the European context.

On August 24, 2017, for example, the Act on the **More Effective and Practicable Design of Criminal Procedure**<sup>10</sup> came into force in Germany. Behind this very clunky name is the ability for authorities to place spy programs on computers. Some call these malicious programs, or “federal Trojans”, because they are able not only to make precise records of the target’s browsing behavior, but also to activate the computer’s webcam and microphone without the knowledge of the person being spied on.

**Read Netzpolitik.org on state run spying software in Germany (In German).**



Of course, one could argue that this type of targeted surveillance is only used in absolutely exceptional cases. This is, after all, also the wording of the law, which states that it is a means of last resort if a crime cannot be uncovered and prosecuted in any other way.

Here, however, as is unfortunately very often the case, legislation lags behind the actual technical possibilities. These specialized programs are not only able to act unnoticed by the target person, they also leave no logs, roughly and simplistically no material that would document their activity at all. Their use would leave no evidence, and there would be no witnesses to be called by a monitored person.

This implies a very important question: who is monitoring the constables? Indeed, the so-called possible “federal Trojan” is by no means unique in Europe, but has already been used as a program in many member states of the European Union.

Who hears the name “Pegasus” might first think of the mythical winged horse, the daughter of the ancient Greek god Poseidon, the symbol of poetry. But Pegasus is also the name of an extremely powerful spy program, a “spyware”, developed by the Israeli company NSO Group. It is considered one of the most powerful cyber-weapons ever developed.

Pegasus is able to infiltrate any home computer and spy on all known messenger services. It is also able to copy users’ address books, query the battery status of devices, record conversations, backup photos and videos, spy on all passwords, find out the location of a device, and even infiltrate clouds.

**Read the New York Times on Pegasus, January 28, 2022. By Ronen Bergman and Mark Mazzetti.**



Several state security agencies of European Union member states have acquired Pegasus and have already put it to use, sometimes without parliamentary oversight. For example, it became known that Catalan politicians were subject to massive surveillance and wire-tapping by Spanish central government security forces using Pegasus, at least in 2019.

The Polish Ministry of Justice acquired the spyware in 2017 and used it to spy on opposition politicians who had been particularly critical of the ruling PiS party. In one case, Senator Krzysztof Brejza, manipulated chat messages were even published on the pro-government public broadcaster, during the 2020 presidential election campaign – extracted by Pegasus<sup>11</sup>.

The same applies to Hungary, where journalists critical of the government were scouted using the spyware. However, the Federal Republic of Germany is also on the list of NSO Group’s customers<sup>12</sup>. For a long time, constitutional concerns stood in the way of procurement by authorities, but in 2021 it became known that the BKA as well as the BND had acquired the program<sup>13</sup>. However, the German government kept quiet about the exact use of the program, which had apparently been “adapted”, before a parliamentary investigative committee. It was only announced that the software was already in use.

However, even at the level of the European Union itself, there is a steady trend toward ever-greater securitization of the private sphere. On May 11, 2022, the European Commission presented a possible new follow-up regulation for the already existing regulation on voluntary chat control by unencrypted providers (GMX, Facebook, Gmail). This is intended to oblige all providers, including encrypting services, to scan and monitor all chats of all users, even without suspicion, for suspicious terms. As one can imagine, Pegasus could also play a decisive role here.

This is justified by an improved fight against crime and terrorism. The objections of numerous NGOs, data protectionists and lawyers that this regulation, if ratified, will pave the way for a surveillance state, are currently falling on deaf ears at the European Commission.

It is never advisable to point the finger at anyone. Nevertheless, one reason for the reckless handling of new cyber technologies by the state and overly quick, ill-considered decisions in the area of cybersecurity by political decision-makers is also often due to a lack of knowledge on their part. Before proceeding to the

analysis of security threats in cyberspace by foreign actors, it is advisable to address worrying tendencies in our common house of Europe. This is what we have done with this chapter.

An important question that arises after all these explanations is: Does it cause any advantage for the law enforcement agencies to store IP addresses and access times? The answer is sobering: little. Although it is very easy to determine the identity of the computer, as well as the time of use, it is not perfectly verifiable who actually used the computer. The relevant laws can hardly be used for anything else, i.e. for comprehensive surveillance measures.

This Policy Report takes an important step towards informing yourself about this issue in more detail. On the one hand, a securitization of public concerns is understandable in the wake of ever new threats, but it must not become self-perpetuating and thus curtail democratic freedoms.

### Sources and Further readings:

**Additional Protocol to the Convention on Cyber-crime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems:**




**Statewatch – Monitoring the State and Civil Liberties in Europe:**



**Europol EC3:**





No one is an island...anymore. In the age of digital networking, the world has “moved closer together”, but what does this mean? Opportunities and dangers have not only become more diverse, they are also “closer” to us through cyberspace.

# 5 How do international online disinformation and cyber attacks affect and threaten Germany, the EU and NATO?

Cyber threats are manifold and are no longer limited to simple hacking or paralyzing websites. With the Internet of Things (IoT, see chapter 1), attacks are possible that can have concrete consequences for infrastructure, machines and also the functioning of the economy and important social processes.

These can affect Germany, but also the EU as a whole but also international organizations such as NATO, the UN, or Interpol.

But first: What is a “threat” from cyberspace anyway? Currently, the word “threat” is used inflationary when talking about Internet phenomena. This leads to some blurring in the debate. In many cases, these are phenomena that have not been properly understood. This leads to them being presented in the wrong proportions – some are overestimated, others neglected.

We use a pragmatic approach to this issue here. **A threat is measured by the real, immediate damage to the integrity of data, devices and people that can result**

**from manipulation from the Internet. It further has a long term effect, which is a loss of trust, insecurity and avoidance.**

It is necessary to distinguish between intended and unintended damage. For example, if a hacker group seeks to block a bank’s server systems with a ransomware, it is an intentional harm. On the other hand, it is an unintended one in the case of an engineer in a grid company who accidentally cuts off power to a part of a city. Natural disasters, such as solar storms, also fall under this aspect. In this report, however, we will focus on the intentional damage to data, equipment and people. It is estimated that there are 2328 cyber attacks each day, or about 849.720 per year<sup>14</sup>.

#### **Damage dimension:**

Any damage caused by cyberattacks has different scopes and impacts. A local attack on a single company, for example, can of course be catastrophic for that company, but hardly affect the overall economic structure. In this case, one can speak of a local dimension. If,



Figure 9: Top 7 Cybersecurity threats to prepare for in 2030. Courtesy of ENISA

however, a chain reaction results, for example from a production stop at a supplier of car parts, this can have dramatic consequences. We want to use the term multilateral dimension for this. A cyber attack on a country's critical infrastructure, such as the power supply, has an impact on the overall integrity of the state; the term global should be used for this.

### Threat vectors

Each potential target has different points of attack, weak spots. The term vector here is deliberately borrowed from biology, as is the term virus for malware. Backdoors, phishing and Trojans, or deep fakes and fake news are not the end goal, but the means for hackers, saboteurs and online propagandists. The more of these possible vectors an entity, i.e., a state, a company, or the like, has, the higher the overall threat.

### Controllability

This term is intended to assess the controllability of events in cyberspace. To what extent do the participants have power over what happens? Can there be a threat of a cascade effect? Here, the attacker side is referred to as hostile controllability and the attacked side as defensive controllability.

### Threats and their significance

We would like to try to give you an overview of the threats that exist, graded according to the explosiveness and danger of these phenomena – separated into cyber attacks and online disinformation.

Since it is not possible to deal with each possible threat situation individually, the most dangerous scenarios will be treated as examples. However, a hierarchical list will be provided here of the threat levels that exist and how relevant they are, as well as a rationale for this choice.

**1. Power Infrastructure (Electrical Energy)**

Possible perpetrators: States, terrorist groups  
 Target: breakdown of public order, destruction of critical infrastructure  
 Damage effect: destruction and/or impairment of modern civilization  
 Damage dimension: Global  
 Threat potential: High  
 Resilience: Limited  
 Rectification: Possible in the beginning, time is the decisive factor

The energy supply represents the lifeline of the country, without it no production, water supply, health care, traffic control, or communication is possible. An attack on it could cause the state and society to face massive chaos.

**2. Supply Chains**

Possible perpetrators: States, terrorist groups  
 Target: breakdown of public order, destruction of critical infrastructure  
 Damaging effect: Destruction of economic  
 Threat potential: High  
 Damage dimension: multilateral  
 Resilience: Limited  
 Rectification: Possible throughout the way, the more time that passes, the more damage

The complex and highly technological production methods of German industry and commerce depend on smooth processes and deliveries. Nowadays, logistics, orders, inventories and deadline processing are managed, recorded and handled electronically. An interruption of these by hackers, for example, can paralyze production times with a just-in-time model and cause irreparable damage. For example, when glass furnaces cool down, they are destroyed, and this is more possible than ever with the IoT, since the control components of, say, these furnaces are also run by software. Without glass, however, industries such as food, medicine, research, and many others have a massive problem and could suffer permanent damage.

Simple DDoS attacks (see explanation of terms) are able to cripple the Internet portals of supply companies, preventing manufacturing companies from getting the parts they need. Think of supply chain logistics as the little cogs that keep industry running. If these, or only parts of them, are disrupted, a chain reaction occurs.

**3. Military, economic, and intelligence motivated Cyber Espionage**

Possible perpetrators: State actors, multinational corporations,  
 Target: information theft, spying.  
 Harmful effect: loss of technological advantage, weakening of defense capability  
 Threat potential: Medium – mounting on a longer run  
 Damage dimension: Global  
 Resilience: Limited  
 Rectification: Possible throughout, but early detection essential for prevention



Figure 10: cyberthreats and their mitigation in two rotating cycles. Courtesy of balbix.com

Germany is a country of innovation; without scientific, inventive and thus also economic progress, the country is not in a position to be among the leading players in international competition. Admittedly, players such as China no longer rely on stealing innovations directly; they now have excellent developers themselves. However, key technologies are still being researched in which, for example, they still have a unique position, such as modern adhesives. Efforts are also being made to find out where weaknesses exist in the “adversaries” systems, how quickly the defenses react and what is being planned.

#### 4. State administration, democratic structures, E-Governance, confidential personal data

Possible Perpetrators: State actors, terrorist groups, criminal groups.

Goal: Information theft, identity forgery, reconnaissance

Harmful effect: loss of confidential data, infiltration, wire fraud

Threat potential: Medium

Damage dimension: Global

Resilience: Limited

Rectification: Possible throughout, continuous monitoring necessary

Personal data of citizens, such as social security data, foremost health data (medical data sets e.g.), tax office data, law enforcement data and other confidential information are the focus of hackers. In addition, personal profiles on social media are in the crosshairs. However, also documents of parliamentarians, investigative committees and personal information about them are in the crosshairs of cyberattacks.

The reasons for this are manifold. First, stolen identities (“identity theft”) can be used to simulate people on the Internet, for disinformation purposes, fraud and espionage. Stolen credit card information can be used to steal money needed to cross-finance covert operations by intelligence agencies, the so-called cyber-crime-cyberespionage complex (see chapter 7, section on the PRC, and as well our Infobox in chapter 1).

#### 5. Telecommunications

Possible perpetrators: State actors, terrorist groups

Goal: Obstructing and preventing the exchange of information

Harmful effect: disruption of transactions, work processes come to a standstill

Threat potential: Medium

Damage dimension: Multilateral

Resilience: Limited

Rectification: Possible throughout, continuous monitoring necessary

In the 21st century, communication via the Internet is massive. This also encompasses more far-reaching areas than might at first appear. Telecommunication concerns not only the exchange of messages between private individuals, but also between companies, banks, government bodies, emergency services and scientists. The server systems of national communication providers can be attacked and put out of action,

their broadcasting equipment can be damaged by malware, or can be foreign-encrypted with ransomware. These scenarios are possible not only at the national level, but also, for example, in the area of the EU, if several large telecommunications providers of populous states are attacked – for example, in Germany, France, Belgium and Poland at the same time. This would also affect the EU institutions, as well as NATO, because even if these institutions have their own servers, they still need to access the network. There would be massive delays.

#### 6. Data security

Possible perpetrators: State actors, terrorist groups, criminal groups.

Goal: Disruption of governmental and economic work processes

Harmful effect: Blocking, loss of trustworthiness, small but crucial malicious changes, or even deletion of crucial data

Threat potential: Medium

Damage dimension: Depending on attack, global and multilateral

Resilience: Only limited

Rectification: Possible throughout, continuous monitoring necessary, backup data protection

As we explained at the outset, the Internet consists not only of the visible front web, or surface web, a significant part of the network consists of non-visible databases, checksums, archives and clouds – the so-called deep web. A wide variety of institutions and businesses depend on this data, on its existence and, above all, on its reliability. Not only people access this data, for example in government administration or in the healthcare sector. It is also used by machines that query specifications or apply checksums for their production activities, for example.

Trustworthiness is very relevant in technical systems, not only social systems. If people can no longer trust the data you receive, technical systems will become extremely complex if not even impossible.

Falsified data can lead to disruptions in production, which must be halted until the source of the error can be identified. Data blocked by ransomware cannot be used, so a group of terrorists, criminals, or a foreign state could encrypt sensitive databases with a malicious program and only release them again against the fulfillment of certain requirements.



Data security also includes confidential information, such as account data and transaction security. Cyber criminals are able to hack credit cards, redirect transferred money and steal passwords. This poses a massive threat to the economic security of the banking sector and thus to commerce as a whole.

### 7. Online Desinformation und Fake News

Possible perpetrators: State actors, terrorist groups

Goal: Reinforcement of social fault lines, tribalism, polarization

Harmful effect: undermining of social discourse, loss of trust in the democratic state

Danger potential: Medium

Damage dimension: Depending on event

Resilience: Only limited, despite existing programs

Rectification: Improvement of public debate culture and inclusion of opinions

You may wonder why this topic comes last. The reason is that online disinformation and fake news do in General seldomly cause physical damage. Nevertheless, they should not be underestimated in their indirect effect on the population in their opinion formation and thus also on free democratic orders.

Contrary to widespread opinion, unfortunately often conveyed in this way by the media, online disinformation does not attempt to build up new patterns of opinion. That would be far too ambitious and costly. Rather, it exploits social frictions and an already battered debate culture in society and tries to widen these fissures. It seeks to create the impression that the entire state is corrupt and beyond salvation, and that the government is actively fighting its own citizens.

Online disinformation uses every trick in the book: News is either invented (fake news), or actual information is distorted in an alienated context, videos are deceptively faked, fake accounts are used to simulate a high level of approval for content and spread it.

## Sources and Further readings:

**BlueVoyant: 7 Types of Cyber Threats & How to Prevent Them [2022 Guide]**



**European Parliament: Cybersecurity: main and emerging threats**



### Electric Power Grid

**US Department of Energy: Advancing Cybersecurity to Strengthen the Modern Grid.** January 2021.



**#SINTEFblog: Cybersecurity in the electricity grid.** June 15, 2023.



### Supply Chains

**New Zealand Government: Supply Chain Cyber Security.**



### Cyber Espionage

**ENISA: Enisa Threat Landscape: Cyber Espionage.**



**Cybersecurity Threats for NATO**

**NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE):** Cyber Threats and NATO 2030: Horizon Scanning and Analysis. By A. Ertan, K. Floyd, P. Pernik, Tim Stevens. (2020)

**Personal Data**

**U.S. Department of Education – Privacy Technical Assistance Center (PTAC):** Data Security: Top Threats to Data Protection. (June 2015)

**Cybersecurity Threats and E-Governance**

**University of California Northridge:** E-Governance and its Associated Cybersecurity: The Challenges and Best Practices of Authentication and Authorization among a Rapidly Growing E-Government. By Luisa Albertina Razuleu. (August 2018)

**Telecommunication**

**ENISA:** Cyber Threats Outcome in Telecom

**Online Disinformation and Fake News**

**Oxford Internet Institute:** Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. By Samantha Bradshaw, Hannah Bailey, and Philip N. Howard.

**A. Germany****Power supply in the crosshairs – attack on the country's lifelines****Threat vectors:**

- ▶ Generation
- ▶ Transmission
- ▶ Distribution

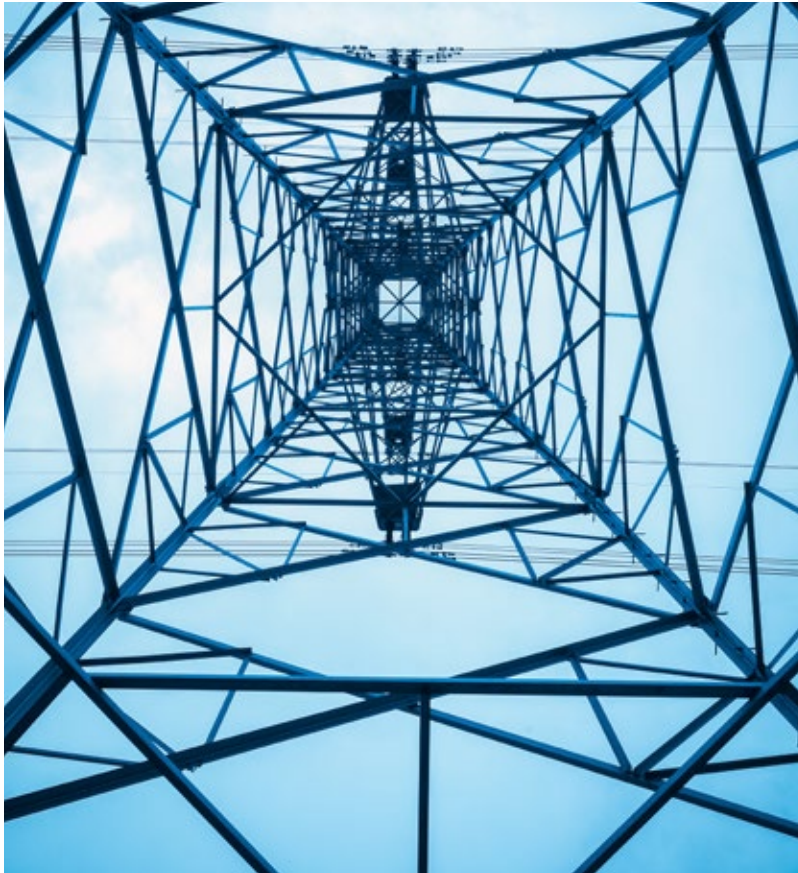
We have all become accustomed to the fact that electricity comes out of the socket. It runs all the important devices, machines and computers that keep our modern, civilized and high-tech lives running. The electric steel furnace in the Ruhr area needs electricity, the street lighting and the traffic lights need it, as do our heating systems, hospitals, water supply and the servers, as well as computers at our work. A functioning power supply is vital for Germany's security.

Behind the supply of this energy is a highly complex, elaborate and sophisticated generation, control and supply structure that must be maintained. In order to simplify the processes, state-of-the-art technology is used here as well: powerful computers equipped with control programs, monitoring functions, maintenance tools, and databases, some of which are connected via the Internet.

This is precisely the weak point for possible hacker attacks, because where digitalized structures exist, there is also a way to infiltrate them and impair their function. The consequences of a large-scale hacker attack on Germany's power supply could be catastrophic and must be prevented.

According to the Federal Office of Civil Protection and Disaster Assistance (BBK), a widespread loss of electricity of just under three days is enough to bring the country to the brink of collapse. Hospitals only have fuel for a few days to run emergency generators, the authorities largely have no such equipment to maintain their radio operations, the failure of refrigeration systems would cause large quantities of food to spoil and cash would be the only means of payment.

The water supply in most major German cities and counties also requires electricity for pumping and purification systems, and without a water supply, sewage systems cannot function properly either. TV, radio and Internet would fail, communication would be very difficult. Gas station pumps would stop working.



Lifeline. Today, we take electricity for granted. Unfortunately, we are not aware that a major outage of this lifeline lasting several days can lead to the collapse of our society and its security.

Research projects, such as biological experiments, could be ruined. Sick people could no longer be cared for and would die, old people could fall dangerously ill in winter due to hypothermia, food would become scarce because the cold chains and transport routes would be interrupted.

After about five days, according to a study by the Austrian army (Bundesheer), public order would have collapsed in the event of a blackout in most parts of the country.

Contrary to this acute threat situation, however, electricity plants and network operators in particular are not protected to the extent that one would expect for such a sensitive key infrastructure. There have also been attempted infiltrations and, in other countries, quite successful sabotage attempts with far-reaching consequences.

A good example of an attempted operation is the infiltration of the electricity supplier Enercity in Hanover in 2022. Although there was no disruption of supply per se, customer service was completely paralyzed<sup>15</sup>. Why

this is not a negligible phenomenon and must be understood in a larger context is illustrated by the following hypothetical example, which also represents the usual modus operandi of such attacks.

Cyberattacks on the power supply invariably target three components:

- Generation (power plants)
- Transmission (high-voltage transfer lines)
- Distribution (substations)

Any disruption in any of these three parts is enough to cause the entire system to collapse. The essential steps hackers must take to accomplish this are:

1. Intrusion
2. Reconnaissance
3. Password farming
4. Lateral movement
5. Place bomb
6. Detonation

By means of fictitious mail messages to employees containing code for infiltration, it is possible to covertly gain access to the computer of one, or more, employees. Even though the office and the control network are physically separated, it is not impossible to overcome this barrier. Covertly, the placed code, which can disguise itself as part of a functioning file, spies out passwords that can lead to further levels, such as servers in power plants and the like. Working routines and employee habits are monitored and analyzed.

Lateral movement refers to the movement of malicious and spy code from one server to additional, multiple facilities within a production process. This means that from a single power plant, an attempt is made to penetrate additional facilities. The malicious code is then placed. It does not even have to be a particularly elaborately programmed piece of software. On the contrary, the more inconspicuous, the better. **Zeroday exploits**, i.e. vulnerabilities in the systems that have been discovered by the hackers but are unknown to the operators, are best suited for this.

The software for controlling the power distribution can be manipulated so that the networks shut down and the programs for it are blocked with passwords unknown

to the operator. The distribution, diagnostic and repair programs can be manipulated so that equipment in the substations is destroyed by overvoltage. The turbines and generators in the power plants can be impaired in their functionality, to the extent that they are destroyed. The smallest manipulation of the 50 Hz grid frequency can damage industrial equipment, cause the grid to collapse. The possibilities are so manifold that they would go beyond the scope of this document.

Another possibility to harm the electric power grid is to create a botnet within a huge number of IoT-devices that consume a lot of electricity. Since the hackergroup managing the attack will be able to take full control of the on-and-off-command of these machines, they could turn them on all together in a moment, when there is high demand for energy on a grid wide level. This can cause a failure of the entire system, since the surge in demand could not be met with production of sufficient electricity. Imagine all industrial, smart-home and logistics IoT devices get turned on in the same moment – the energy grid in Europe, which is already instable, would collapse immediately.

In view of the latent instability of the German power grid, the significance of possible hacker attacks is

The energy supply of enemy states is now the number one target of all military cyber units, but also of terrorists seeking to hit the lifeline of nations.



increasing enormously. It no longer requires a large-scale attack on the entire infrastructure.

In 2019, a grid frequency fluctuation dropped the German power grid to 49,8 Hz, and this was not a single event. Due to the complexity of the systems and the fact that the phenomena cannot be fully investigated, it cannot be ruled out that some of them are due to probing cyberattacks. This trend is not only perpetuating itself, it has worsened massively: from March 27, 2023 to March 29, 2023, there were 10 grid frequency fluctuations – within not even a little more than 24 hours<sup>16</sup>. Since the beginning of Russia’s war against Ukraine, the Russian hacker group Killnet has expanded its activities to harm Western states. It can be assumed that Germany’s power supply has long been in its sights.

In this context, it can be observed that a regular arms race has been launched on all sides to exploit the vulnerabilities of the respective “adversary”. The People’s Republic of China, the Russian Federation, but also the USA are actively looking for ways to plant dormant “time bombs” in the systems of their respective opponents. Is a new “balance of terror” just building up? We will deal with this later in this report.



## Source and Further Readings:

### Office of Technology Assessment at the German Bundestag (TAB):

What happens during a blackout: Consequences of a prolonged and wide-ranging power outage. (2011)



### Austrian Bundesheer: Sicher. Und morgen?

Sicherheitspolitische Jahresschau 2020 (In German: Safe. And tomorrow? Security policy outlook for 2020)



**The Record:** Major German energy supplier hit by cyberattack

<https://therecord.media/major-german-energy-supplier-hit-by-cyberattack>

**The Wire:** How an Entire Nation Became Russia’s Test Lab for Cyberwar



## B. The European Union: repeatedly in the crosshairs from cyberspace

### Threat vectors

- ▶ Crisis situations in the 27 member states
- ▶ Energy distribution
- ▶ Securing the EU external borders
- ▶ Transport network (train, air traffic, ship traffic)
- ▶ Confidential data of EU authorities and thus also of its members
- ▶ Creditability

Like its member states, also the EU as a whole – its political system and citizens – is threatened by online disinformation and cyber insecurities. But in this example, we do not want to focus on the working level of the Union, but on its credibility – a major resource on which the legitimacy of ever political community relies.

Online disinformation is able to attack this credibility and to strengthen and deepen already existing negative attitudes within parts of the population towards the EU.

Further, in this scenario, which unlike the previous one is not fictional, it will be explained how cyber sabotage and online disinformation can be actively intertwined and how the EU itself must also combat internal shortcomings in order to remove the breeding ground for these operations.

As in any political system, online disinformation can hook up to real or exaggerated examples of corruption and mismanagement that might undermine overall trust in the body politics.

The simplest and also most effective strategy to attack the credibility of an institution is thus to use its own flaws against it. This simple and proven trick has worked as long as propaganda has existed and is still applicable today. The world may have become more complex, but the basic principles behind it have hardly changed.

Kremlin propagandists can easily exploit these scandals and aberrations. As we noted in our definition of online disinformation, successful propaganda is rarely a complete fabrication, or a complete lie. They target and reinforce basic mistrust, fears, and assumptions.

Russian propaganda is currently playing out primarily on Telegram, Twitter, and media outlets such as RT (Russia Today) and Sputnik, which can be accessed with ease using a VPN (see definitions), despite all attempts to block them by EU member states.

Through these online media and social networks, basic fears that many citizens have are reinforced. Rarely are there tangible made-up stories to read, or tweets to follow on topics that are completely lies and confabulations. However, their interpretation is altered and destructive intent is brought across in an argumentatively credible way.

The narrative should sound familiar: The EU, for example, is developing into a tyranny in which omnipotent commissioners decide what they want without any accountability and disenfranchise the people. The transparent citizen is to be created, while the elites would plunder the people. This is the common narrative on Russia's disinformation networks. Particularly sophisticated here is the system on which discursive loops are produced, constantly reproducing themselves and creating the illusion that different people and groups would discuss the content interactively. In this way, credibility is simulated despite the fact that



News at a click. But how much is good quality information and how much is just an attempt to unfairly manipulate our opinions? In this day and age, with all its speed and lack of focus, this difference is often not easy to recognize.

they are controlled semi-automated bots – fictitious online profiles of people who look real through deep fake images and respond to content pre-produced by media loyal to the Kremlin.

However, media outlets such as RT and Sputnik, as well as the semi-automated bots, are under the control of the GRU, Russia’s military intelligence agency and affiliated companies – in a state whose population is itself held hostage to the authoritarian, anti-democratic regime ruling the Russian Federation. The “Internet Research Agency” a semi-governmental company based in Saint Petersburg, actively and meticulously operates these semi-automated botnets, but as recently revealed, behind these activities is an even larger complex: Vulkan (more on this in the next chapter).

The following example is fictitious, but it is representative of many cases of Russian disinformation on the Internet:

*Let us assume that you are following a certain hashtag on Twitter that is currently “trending”, i.e. a topic that is currently being heavily discussed. Let us call this hashtag #euparlamentcorruption. One user, let us call him @realmichaelscott, who seems to have a high reach, tweets about the corruption scandal, but sprinkles in some “previously unknown information”. What you are not aware of is that it is a Russian bot and that while the commonly known facts are correct, the “special information” is pure fabrication. However, you do not inquire further, after all, several hundred people seem to follow @realmichaelscott, he himself also has quite authentic personal information and a profile picture. However, most of his followers are also semi-automated bots, profiles of people who do not exist in reality, but give the impression that it is a natural, organic discussion with significant reach. A technique which is called -> Astroturfing.*

*Some of these followers interact with @realmichaelscott and comment with links to the account’s tweets. There are even websites from daily newspapers among them that you also read. After you click on it, you read an interesting article, but it was created on a fake website that deceptively resembles the original. This way, you get the impression that the information is authentic. This happens not only to you, but to thousands of users on social platforms. The effects of this strategy are two-fold: Either you believe the information and follow the link trees, in which case you are “in the rabbit hole”. The second variant is that they recognize that it is misinformation (through attentive analysis of the information,*

*through fact checkers, etc.) and follow news, as well as the discussion on the net, only with profound distrust.*

So, as you can see, the perpetrators cause potential damage in two dimensions through their strategy: decreasing trust and dividing society. However, defensive protagonists unfortunately also play a role in this game. The more political scandals increase, such as corruption around members of the EU Parliament, for example, the easier it becomes to damage the credibility of the entire Union propagandistically. This is the reason it doesn’t help much to ban media and sites, and to put most of the money into fact checking, if the fundamental problem is not eradicated.

Added to this is the increased vulnerability of the EU due to its supranational structure. Let us just recall for a moment the possibility of hackers gaining access to sensitive data, of the population, of institutions and the like. When confidential documents are leaked, accompanied by a massive disinformation campaign, this can lead to a real political earthquake.

## Sources and Further Readings:

**EU vs. Disinfo:** New Website with Disinformation Database.



**University of Massachusetts Amherst:** Fake News and Scandal. By Jason Cabañes, C.W. Anderson and Jonathan Corpus Ong. (2019)



**Tagesschau:** Fake-News-Jäger in der Kritik (In German: Fake news hunters under criticism)



## C. NATO – In the trenches of digital armament.

### Threat Vectors:

- ▶ Defense Plans
- ▶ Command and Control Systems
- ▶ Classified Information
- ▶ Espionage
- ▶ Communications

As a defense alliance, NATO is exposed to many potential sources of danger. NATO is less exposed to the undermining influence of online disinformation as (supra-)national polities such as the EU or Germany. NATO's character as an international organization bears different threat vulnerabilities. The threat from cyberspace is a relatively "new" one for them as well, and adaptation to the situation sometimes lags behind technical developments. One aspect in particular is of special importance here, the command and control systems.

The case of the Orion platform from the U.S. company SolarWinds in 2020 showed that centralized organizational and logistics systems are particularly vulnerable to targeted cyber espionage attacks. SolarWinds' innovative products have been widely deployed, for example in the US administration and also in NATO. Hackers managed to exploit a backdoor in Orion that remained in place even after updates to the system and gained access to sensitive data from the U.S. Department of the Treasury, the U.S. Department of Commerce and the U.S. Department of the Interior, and there are also suspicions that the EU Parliament and NATO could be infiltrated.

The originators are very likely based in Russia and are part of a comprehensive complex in the the **Vulcan network**, which combines the capabilities of Moscow's intelligence services and private companies.

As NATO announced in 2020, no compromise of its system software could be detected. Nevertheless, an extensive hardening program has been initiated to eradicate the possibility of backdoors being exploited. But what threats exist despite all the precautions? NATO uses software at the command and control level, these are not (yet) unified on a per base basis, yet they are individually vulnerable. These include airspace surveillance systems through the network of radar stations, such as Multi-AEGIS Site Emulator. This is not

only capable of monitoring its own airspace in a network of local radar operators, but also of looking deep into enemy space to detect approaching aircraft.

Bi-SC AIS is a system that effectively transmits military messages and enables hierarchies within NATO to communicate with each other more easily and quickly. However, both systems are computerized and this makes them vulnerable to external attacks, whether for sabotage or espionage to find out the exact positioning and knowledge of defense readiness. A compromise of these key systems could lead to manifold damage. The loss of radar surveillance would make it possible to penetrate NATO airspace without warning, and it might subsequently be too late for effective air defense. Interceptors would not rise in time to counter threats. Germany's air defenses, which in any case have limited operational capability – the IRIS and Patriot batteries are only sufficient to protect a few neuralgic points – could be destroyed on the ground while still inactive.

Interfering with the alliance's direct communications capabilities targets a weakness of military institutions that is not directly located in the technical domain: the hierarchical structure of chains of command. The entire communications system need not be affected at all; only some of the highest command posts would have to be separated from the rest, and the alliance would have difficulty coordinating defenses effectively. This seems relatively unlikely at present, but it is still worth looking at recent history to illustrate how hacker groups could cause such damage undetected.

The Stuxnet affair has shown that time need not be an immediately decisive factor for state, or even terrorist, actors. The virus, which presumably originated in a special cyber unit of the Israeli army, was spread in a rather unconventional way: Through mails and through USB sticks.

Iran's Natanz and Bushehr nuclear facilities, like all high-security areas in any state, are organized "air-tight." That is, they are physically separated from the Internet so that no direct attacks are possible. However, as Stuxnet demonstrated, with a little patience, impact is possible. It spread primarily through e-mail traffic until a certain "saturation" was reached, which allowed the virus to jump to USB sticks.

One of these infected USB sticks found its way via an employee who (unknowingly) connected it to an internal computer at Bushehr. The rest is history, so to speak; a large number of the uranium enrichment cen-



trifuges were severely damaged. A simple overclocking of the rotation speed put the sensitive equipment out of commission.

This lengthy but steadily creeping and subliminal process targeted a single technological application and managed to overcome the “airtight” principle. This means that a mere disconnection from the “Internet of Things” (see Definitions) might not be sufficient, insofar as the time factor is not directly important for the adversary.

It is unrealistic in the 21st century to demand that governments, companies, or civil society take things offline that have already been digitized. Rather, developments point in the direction that digitization is irreversible and has created a gravitational pull that is drawing more and more aspects of our daily lives, economies, and politics into virtual space.

A good example of this is, for example, the U.S. Department of Defense’s effort to establish rapidly responsive Joint All-Domain Command and Control systems in order to be able to establish an effective defense in the event of an emergency. The individual computers and servers are not only connected via a digital network, they are also optimized by artificial intelligence. Other countries will at least catch up to avoid being left behind in this development.

Nevertheless, there is still one segment of the military sector that continues to rely on “obsolete technology” and has thus become virtually unhackable: the nuclear arsenal of the United States. The computer centers of the weapons silos date back to the 1970s and were only upgraded by floppy disk drives in the 1980s.

An outdated, specially developed programming language called COBOL is used, which today is only mastered by selected specialists. It is now quite difficult to recruit new personnel who are familiar with this unusual technology, which should actually be considered obsolete in the aspect of progress.

Nevertheless, there is immense strength in this supposed “backwardness.” The computer systems at the main ICBM nuclear weapons bases in the northwestern United States are virtually invulnerable to hacker attack. They are not connected to any network, no viruses or malware exist for the niche product software, and there are no external entry points because floppy disks are no longer in use.

Although there are always voices calling for modernization to today’s standards, this has not yet taken place. This is a welcome development because although,

of course, once technology has been digitized it will never go offline again, it is possible to keep highly sensitive areas offline forever.

The benefits of modernization in the area of nuclear weaponry do not exceed the costs that would be incurred. Just imagine if the control, targeting, and launch systems at ICBM bases in Wyoming, Montana, and North Dakota could be infiltrated and manipulated by hostile hackers. The result, in the worst case scenario, could be the triggering of World War 3. That is why it is advisable, even for the European nuclear powers France and Great Britain, to keep their systems off the grid.

## Sources and Further Readings:

**Cyberthreat.Report:** Russian hackers disrupt NATO comms used for earthquake relief. February 14, 2023. By Katalin Béres.



**The Guardian:** ‘Vulkan files’ leak reveals Putin’s global and domestic cyberwarfare tactics. March 30, 2023. By Luke Harding, Stiliyana Simeonova, Manisha Ganguly and Dan Sabbagh



**Chatham House:** Cybersecurity of NATO’s Space-based Strategic Assets. July 01, 2019. By Dr. Beyza Unal.



**Maxwell Air University:** Nuclear Deterrence in Cyber-ia Challenges and Controversies. Fall 2016. By Dr. Stephen J. Cimbala.





The dragon – a central motif in Chinese mythology and a symbol of the country. The central aspect of this figure is power and the ability to bring it to bear in any location.

6

# Has the digital dragon awakened? The People's Republic of China and its plan to become a cyberworld power

“Let China Sleep, for when she wakes, she will shake the world” Napoléon Bonaparte is supposed to have said. Today in 2023 it seems that this is the case, the People's Republic of China is not only the (by now second) most populous country on earth, but also one of the strongest growing and largest economies in the world and ranked third in the world's military power rankings.

The European Union, above all Germany, has intensive trade relations with the “Middle Kingdom” and many of our everyday objects are already produced in Shenzhen, Guangzhou, or Fushan, and Hong Kong and Shanghai are vibrant financial metropolises with innovative research centers. In 2022, the EU's most exported commodity to China was machinery and transport equipment, totaling around 120.1 billion euros<sup>17</sup>.

However, this emergence is also associated with an aspiration on the part of the leadership in Beijing. The People's Republic wants to become a great power and establish a hegemony in East Asia that clashes above all with the interests of the United States in the region.

This also includes the massive expansion of capacities in the area of offensive and defensive capabilities in the cyber domain, as well as an intensification of information warfare on Beijing's part.

### Grand Cyber Strategy 2017

The PRC is not a country with a liberal-democratic order. It is an authoritarian state with a hierarchical structure. The Chinese Communist Party (CCP) is the only party in existence and allows social discourse only within the very narrow limits it defines and controls. Only the economy enjoys a certain freedom of action, as China has a seemingly paradoxical hybrid of communist one-party rule and a capitalist market economy.

This also has crucial implications for cyberstrategy and its implementation by the People's Republic of China. Ignoring the lack of bourgeois democratic freedoms, this form of government also has a procedural advantage for the implementation of projects: Speed.

Since there is no separation of powers, no checks-and-balances, there are no appeals, no public review, and no democratic negotiation of decisions once made by the CCP leadership. This means, in purely sober terms, that the People's Republic of China could and can implement its decisions, with respect to its cyber strategy, more quickly than is the case in the European Union, for example.

In 2017, Beijing made it clear: a new cybersecurity strategy is being developed, based on three pillars.

### The Three Pillars:

- expanding cyber military and warfare capabilities
- limiting the threat of the internet to Beijing's hold on power which extends to domestic information control
- shaping global cyberspace norms to extend China's influence

A core concept that is crucial for the understanding of Beijing's strategy is **data security and sovereignty** as it is called, and which includes cyber warfare and norm-building capabilities. This concept is directly linked to the expansion of the People's Liberation Army's military clout in the field of active cyber warfare and the defensive protection mission of the armed forces. This is because the People's Republic's cyber security is not under the control of any civilian agency, but directly under the military.

Six years ago, in 2016, the People's Liberation Army was drastically reformed. One step was to downsize the armed force, and to invest in more efficient units, one of them was the new created Strategic Support Force as part of the land forces.

The newly created component force has competencies in the areas of:

- Space warfare (satellites)
- "political" warfare (disinformation)
- electronic warfare (telecommunication systems, reconnaissance)
- Cyber warfare (digital information, data protection, network security, espionage)

The marching song of the component force says a lot about the self-image of this newly created formation, as well as the perspective that prevails in the Chinese leadership on the subject: "We Are the Knife Point, We Are the Iron Fist".

But there is more to the component force than meets the eye. It is a so-called stovepiping principle, also known from the intelligence field. The individual agencies and services of security organs tend to operate only "along a tube," hence the term, i.e., only within their own house and ministry and hardly cooperate with other institutions in the state. This is due to the strict rules of secrecy, confidentiality, legal requirements

and regulations, but also often due to the distrust that individual state bodies often have of each other.

Stovepiping does not have to be negative, however, depending on which higher-level agency sits at the end of the "pipe." The Strategic Support Force was created for precisely this purpose. It combines intelligence, military, and "political" reconnaissance into one component force.

The politicized language of the People's Republic of China does not speak of "hybrid conflicts," "hybrid warfare," or cyberwar. They call these kinds of international disputes "informationized conflicts" and also do not separate online disinformation from cyberattacks, such as hacking, but see this as a single entity. For this reason, "political warfare", i.e. disinformation, and cyberware units are also housed in the same "house", so to speak, united in the army. For this report, one subdivision in particular is of interest: Network Systems Department (Cyber Warfare).

This subdivision is in turn divided into various sub-units, such as:

- **Unit 61398** – Specialized in hacking and spying on foreign military
- **Unit 61486** – Specializes in hacking in the area of industrial espionage, primarily by infiltrating communications technology
- **Unit 61726** – Cyber unit focused primarily on activities against Taiwan
- **Unit 61786** – Responsible for the monitoring of telecommunications in Central Asia and Russia
- **Base 311** – Center for psychological warfare, opinion manipulation, and legal challenges in the digital realm
- **MSD 56th Research Institute** – Software and hardware development, the first supercomputer of the People's Liberation Army with 100 GHz processing power was constructed by this institution. For comparison, the strongest commercially available processor for personal PC from AMD currently has a maximum power of 5.7 GHz, from Intel 5.8 GHz.

Interestingly, there is also a training institute associated with the Network Systems Department: the Zhengzhou Information Science and Technology Institute, which itself does not have a military designation in its title. There, students who are themselves soldiers are trained in technology, cybersecurity, espionage, infiltration and psychological warfare.

In addition to all these “official” cyberwarriors, there also exists a wide range of cyberwar structures that can be described as “paramilitary” and thus not only fit into the Maoist doctrine of unity of “theory and action.” The Ministry of the Interior, i.e., state security in the People’s Republic, also maintains its own cyber departments. However, these are “PLA authorized,” meaning that they act under the supervision of the armed forces by authorization. There are also “independent civilian” hacker groups. Individuals who ostensibly take the initiative “spontaneously” for patriotic reasons. This is doubtful, however, because here, too, only the interests of the Chinese leadership are expressed, which would be difficult to argue diplomatically.

The Network Systems Department also has its own state-owned company, China Electronics Technology Group Corporation. This company produces its own hardware and software in the fields of communications technology and data processing for civilian and military applications and thus also has a decisive influence on the so-called cyber sovereignty of the People’s Republic. Beijing aims that successively only hardware and software licensed and authorized by Beijing itself, as well as social media, are to be used in China and by foreigners if they make business on Chinese soil or with Chinese technology. Of course, this is all done under the pretext of national security and quality control, but on the other hand, of course, also to ensure the complete monitoring of all telecommunication channels and devices. On the other hand, this circumstance also makes it much more difficult for Beijing to prevent foreign espionage attempts that target technological vulnerabilities.

Another pillar rounds off the strategy: the securitization and standardization of the legal framework for commercial data in the People’s Republic of China. This provides that every entity, i.e., physical and legal persons (companies, for example) that are active in China and generate information there must also automatically store this data within the country’s borders. Although this only applies to so-called “important

*“So there are two aspects to this thinking if you’re Beijing – one, you don’t have to rely on foreign suppliers to ensure your own security and you’re more aware of your own vulnerabilities, with limited supply chain entry opportunities. Two, that important information is within the state’s own infrastructure, and the state, in that way, is also able to maintain control and knowledge over the information.”*

Tiffany Wong, Director, China Practice Director, China Practice, Albright Stonebridge Group

data”, it is not defined more precisely which data falls under this definition and which does not.

This not only makes it possible for security agencies to access, monitor and control this data at any time. It also gives Beijing the ability, for example in the event of an international trade dispute, to block the commercial data it needs and thus exert pressure. This type of sanctioning has already been used by China, for example against Lithuania after the country allowed Taiwan to open an embassy. This had economic consequences not only for Vilnius, but also for the surrounding states and the entire EU.

This brings us to the “active measures” of the cyberwarfare forces of the People’s Republic of China and how they have already affected especially Germany, Japan and international tech companies.

## The Game: Chinese Cyber Espionage

Germany has been the focus of cyber espionage activities from Beijing since at least 2007. It is important to note that the illegal activities are “only” limited to the area of cyber espionage. There have been no attempts to disrupt critical digital infrastructure or hinder its work. It is also important to note that despite all efforts and attempts to determine and “nail down” the state origin of programs and groups of perpetrators, this is not possible with definitive certainty even in the case of “Chinese” hacker attacks. This is the problem of the so-called “attribution” which we will discuss later. Here, however, we shall proceed further under the assumption that the cyberattacks actually originated from the PRC, or from groups associated with it.

The Chinese hackers are interested in stealing technological innovations, gaining insight into the state of research in the field of defense technology and obtaining secret economic data. In doing so, “civilian” hacker groups are primarily resorted to, as in this way any responsibility on the part of the Chinese authorities can be denied in the event of detection.

The means of choice are often so-called Trojan horses (see explanation on page xyz), which are deliberately placed by Chinese hackers on company computers and servers. This can be done in various ways. One of the earliest and also still most common methods is sending supposedly serious e-mails containing a worm. However, it can also be serious mails from a legitimate sender who is not aware that he has sent manipulated files. This is not (yet) the Trojan itself, but as soon as the mail is accessed, the worm loads the virus itself onto the computer.

Once the spyware has reached its destination, it is able to spy on servers, transfer data. This includes sensitive files, such as sensitive research results, secret information and employee files. Various German companies have been affected by this in the past, sometimes several times:

- 2012: EADS (aerospace and defense), ThyssenKrupp (steel industry conglomerate)
- 2016: ThyssenKrupp
- 2019: Bayer AG (chemicals), BASF (chemicals), Siemens (conglomerate), Henkel (chemicals), Covestro (chemicals)

In order to understand the infiltrations well, the following criteria are crucial when considering them:

1. what are the targets of the attackers?
2. what are the necessary and sufficient conditions for Chinese hackers?
3. what is the modus operandi?
4. can attribution be successfully performed?
5. what are possible countermeasures?

### Exemplary: The “Winniti” system

Time and again, the focus is on one particular hacker group that keeps Western security agencies on their toes: Winniti. According to current knowledge, this is a group of private individuals who operate with their own programmed malware and whose origin, accord-

ing to the BSI, is in the People’s Republic of China. The focus of the hacker group was mainly German companies in the chemical industry, but also software companies offering critical key services and, to a lesser extent, espionage against critical students in Hong Kong.

A key characteristic of the grouping is that, according to all information, malware and people form a single unit, a symbiont, so to speak, of hackers and software they have created themselves. The “trick” of Winniti is that they send out fake update offers, for example for anti-virus programs.

#### What is striking here is that Winniti camouflaged its actions (almost) perfectly:

Since the individual codes that programs need to run on a system are very extensive, they are centrally organized and unified in a so-called DLL library. This saves memory space on the respective computers. These shared codes are provided with a security signature, which proves the authenticity of a respective file, library etc..

Winniti was, or still is, in possession of stolen, or excellently duplicated security signatures, which are used in the case of their malware in order not to be objected to by defense programs.

An important feature of the work of collectives such as Winniti is that they start their work in a very small way, unnoticed and initially in inconspicuous domains of the Internet. As far as is known, the group first targeted popular online computer games in order to obtain the first security signatures there, and then used these already stolen signatures to obtain more, newer and stronger security signatures.

But what is the difference between military hackers acting on the orders of a state and organized crime?

**In short, it could seem that cyber crime and cyber espionage are one and the same – but still, they are not.** Cyber Crime is often a necessary condition for successful actions in the field of espionage, because without the right keys (security certificates, encryptions, passwords, etc.) it is very difficult to penetrate networks – obtaining them is possible only through criminal activities. Yet, the difference in between pure cybercrime and cyber espionage are the motives and the perpetrators (-> chapter 1 Cyberspace Taxonomy).

## HAS THE DIGITAL DRAGON AWAKENED?



No other country is more frequently associated with industrial espionage in cyberspace than China. Beijing is no longer the only player in the field of industrial espionage, but it is still the most active and also the most successful.

In part, Winniti also sold stolen certificates itself on the black market, but the group's main target was primarily German chemical companies. Attempts were made to send mails with deceptively genuine requests for due updates to employees of BASF, Bayer, Henkel and Covestro by circumventing security barriers (virus protection, firewall, etc.).

This endeavor was also crowned with success, it is enough that only one of the users opens the corresponding mail to bring the Trojan to its target, the PC and the company server. As soon as the spyware arrived at its destination, it sent a so-called beacon, a short signal, to the group that it had reached the right place (server, drive, directory).

By placing malware, Winniti's hackers also had the opportunity to manipulate other files on the servers of these large companies and rewrite them for their own purposes.

However, in doing so, they also leave traces in the files they manipulate, which can be traced by cybersecurity companies and government institutions. The affected German chemical companies, but as well engineering giants like Siemens, claim that the intruders were detected early on and that further damage could be

averted. However, all of the affected companies are keeping a very low profile about the actual consequences of these security breaches, which is understandable, since it can have a very negative impact on a company's ability to do business if its partners discover that confidential and sensitive data is not safe with the company in question.

However, Winniti is not only active in Germany, although the Federal Republic is a focus country. There were also espionage attacks by the hacker group on Japanese chemical companies, as well as an unsuccessful attempt to infiltrate the Teamviewer company from Göppingen in 2016.

This incident must set all alarm bells ringing. The company offers so-called remote services for companies and private individuals, i.e. remote control and remote maintenance of computer and server systems. This is a very practical tool that allows a company's IT specialist to conveniently access the computer of an employee who has a problem, for example, from headquarters.

However, it is impossible to imagine what could happen if hackers were able to gain access to the 2 billion end devices on which the service is installed via the Teamviewer application. It would be a gateway not only

*“Huawei’s office in Serbia was opened in 2007 and has since served as a hub for the whole Western Balkan region. Huawei is a commercial user of Serbian National Data Center, and one more state-owned data center in Kragujevac. Huawei signed an agreement and provided a grant to Serbia for the development of the AI platform and cloud infrastructure for the National Data Center. Additionally, Huawei funded the Kragujevac City Data center – providing a grant of \$2 million for the needed equipment. Finally, in September 2020, Huawei officially opened its Digitalization and Innovation Center in Belgrade. In addition, Serbian state-owned telecommunication company, Telekom Serbia is procuring equipment, services, and infrastructure from Huawei.”*

Dr. Vladimir Ajzenhamer, Assistant Professor of International Relations,  
University of Belgrade, Faculty of Security Studies

to Germany’s industrial companies, but also to the servers of banks, research institutions, political parties, associations, and the media.

But what about attribution? Can one really be sure that Winniti is under the control of the PRC? Unfortunately, the answer is sobering: No. This is due to various reasons and the insufficient possibilities to accurately attribute and locate the actions.

Normally, when analyzing analogous clandestine operations, an advisable *modus operandi* is to first look at where the financial means for carrying them out come from. In the case of Winniti, this is very difficult, as the group’s funds come from cybercrime activities. The group hacked platforms of Internet games where users can win money and had enormous sums paid out to them through manipulated accounts. They sold stolen security certificates on the black market and these are just some of the known activities.

So the money itself is not directly from Chinese authorities, it is not even money that was laundered, it is money stolen directly by Winniti. But how was a limited attribution still possible?

- 1. Chinese characters appeared in the individual tools discovered, which were used on the servers and computers of the affected companies**
- 2. A hacker was actively recruiting in relevant forums for comrades-in-arms for a coup in Germany**
- 3. The activities were committed at times that are indicative of East Asian time zones**
- 4. The extent of the hacking and the infrastructure required for it point to the conclusion that it was carried out by a state or state-controlled actor.**

Is this enough to say with certainty that it is a hacking group under the control of the government in Beijing? Unfortunately, no. Because, as Mustafa Isik, Computer Scientist and Software Engineer has already stated, it cannot be said with conclusive certainty that these are hackers from the People’s Republic. The relevant attribution information may also have been fabricated by a third party to put the blame on Beijing.



This was also underlined by a member of an intelligence service of an EU state, who did not want to be named further, in an article for Bayerischer Rundfunk (BR):

***“If I wanted to hack anyone right now, I’d make it look exactly like a Chinese group.”***

A thought that should definitely be kept in mind.

### **What conclusions and recommendations for action can be drawn from these observations?**

We can therefore conclude that the focus of Chinese hacking activities is clearly in the area of industrial espionage. Further that also the modus operandi is based on a highly complex system with multiple concealment mechanisms and integrative fields of activity from the areas of cybercrime and cyber espionage.

Of course, it must be mentioned that the People’s Republic of China is also making attempts to influence various debates on Twitter. As the Oxford Internet Institute also noted, there is sufficient evidence to suggest that fake accounts are being used to try to simulate debate, primarily to put diplomatic missions of the People’s Republic abroad in a better light.

However, these efforts bear no relation to, say, Russia’s efforts to influence public opinion in other states, nor do they reflect the PRC’s strategic self-image.

Within the framework of its Belt and Road Initiative, Beijing is relying on a principle that is also familiar in the EU: change through trade. A glaring example of this is the Republic of Serbia. Under the initiative, there is massive technology transfer, increased foreign trade and direct investment – with annual increases. This is happening without the use of propaganda campaigns, such as on social networks.

Technological backdoors also play a role here, the possibilities for espionage. Serbia plans to purchase large servers for the digitization of the state administration from Huawei. As we pointed out at the beginning, Chinese services use self-developed software backdoors to get into specially produced systems. For example, the Huawei server infrastructure offers Beijing the opportunity to directly spy on the administration of the Republic of Serbia.

In the case of Serbia, this is probably more a matter of being able to siphon off intelligence more easily than economic espionage. Even the second has changed decisively in recent years, as the exemplary Winniti case demonstrates very well. There is no longer an indiscriminate attempt to grab patents and innovations, as may have been the case in the past.

The People’s Republic of China now has a leading research base itself and is only trying to catch up in selected niches. This becomes clear with the presumably targeted targeting of the chemical industry in Germany and Japan.

*“At present, the dominant norm of cyberspace behaviour is ‘do anything, deny everything’. This is led by Russia and China but is also nourished by the post-Snowden hangover of historical Western misbehaviour. It is time to make a definitive break, both with Russia and China, and with the uncomfortable legacy of the digital surveillance practices of a decade or more ago. This speaks to the second problem.”*

Dr. Tim Stevens, Head of the King’s Cyber Security Research Group,  
Kings College London

Hardly any other country has such a pronounced and sophisticated surveillance state as China. However, the communist regime does not need telescreens or helicopters, as in the dystopian novel 1984. Total surveillance runs almost imperceptibly in the background.



**The following steps are recommended in dealing with Chinese cyber espionage.**

**State Level**

**Technological normative:**

- Tit for Tat – the compulsion on the part of the Chinese authorities to use only local codes and tools in the activities of companies within the People’s Republic can also be applied vice versa to the scope of European law. Only software products that have been either developed or approved by European agencies may be used in the Union by all parties.
- To ensure this process, software companies must have the openness to allow the relevant authorities to see their code. The Chinese state itself develops the relevant programs, codes and tools in order to retain full control over the digital infrastructure at the national level. This is difficult to implement in a liberal democratic society, but at least contractual, trust-based cooperation can be implemented. Between state authorities and companies based on the implementation of a good of common interest, the greatest possible security, these can establish reliability and trust between all economic partners and better combat espionage.

**Intelligence Operational:**

- Strengthening intelligence capabilities in the area of active source hunting and information gathering. As the Winniti case shows, the hackers move around in relevant forums, most of which are probably on the darknet. Synergies between cyber espionage and cybercrime are also visible there, and they go hand in hand. Not only improved technological analysis of attacks is necessary, but also active reconnaissance of activities in the relevant “scene” and on the black market. In other words, classic intelligence information work and an improved possibility of “connecting the dots.”

**Business Management Area:**

- In the area of corporate management, it is advisable to strengthen employees’ sensitivity to the trustworthiness of data. The human factor and individual errors are often the first gateways for hackers and espionage activities. Mails should be viewed with general skepticism; even inconspicuous and authentic-looking mails may in fact come from a hacker group and contain malicious code.

## HAS THE DIGITAL DRAGON AWAKENED?

- System administrators must keep their suspicious code detection programs up to date.
- Companies should be guided to establish a shared confidential database with other companies to share information regarding suspicious activities, stolen codes, forged security certificates, etc.

### Further Readings:

**CISA (US Cybersecurity and Infrastructure Agency):**  
China Cyber Threat Overview and Advisories



**Carnegie Endowment:** What Are China's Cyber Capabilities and Intentions?



**Sinolytics:** Navigating China's Cybersecurity and Data Protection Policies





The matryoshka is a famous object of Russian folk art. These are artistically painted figures that fit into each other in ever smaller sizes. It is a similar story with the Russian secret services, through which a large part of Moscow's cyber potential is organized. Intricate, inscrutable and always designed for surprises.

# 7 The Russian Federation: information warfare and cyber sabotage – “designated battle-fields” as understood by Moscow

---

Russia has a long tradition in strong and extensively equipped military and civilian intelligence apparatus. Although the sheer size of these institutions and their power endowments seems incredible, it should be noted that not all branches of the various services are, of course, used for foreign sabotage, propaganda, or infiltration.

Nevertheless, there is a significant difference with the cyber activities of the People’s Republic of China:

- 1. Russia actively uses digital measures on a larger scale to influence public opinion in various countries**
- 2. unlike the People’s Republic of China, Russia has already deployed parts of its arsenal in the military field for cyber sabotage in the ongoing Russian war against Ukraine**

The Russian Federation is a global actor that has repeatedly attracted attention in the past with spectacular manipulation and attack attempts from cyberspace. Moscow’s intelligence services the GRU, FSB, FSO, SVR all maintain at least one unit, or department dealing with cyber affairs. The term disinformation is a neologism that first appeared in a Soviet KGB manual, “Дезинформация” (dezinformatsiya), where it des-

cribes “false information with the intention to deceive public opinion.”

The foreign policy line of the Russian Federation is understood in a permanent threat situation by the European Union, the NATO and above all the USA – these would seek to destroy and dismember Russia. This legitimizes, in the view of Moscow, the use of extreme means in the area of armed forces, intelligence services and diplomacy in order, as it says, “to secure the interests and continued existence of the Russian Federation.”

The reason for this martial view, however, is also the domestic political upheavals and contradictions within Russia. Vladimir Putin, president of the federation for eighteen years, did lead the country out of the deep crisis and disruption of the Yeltsin era at the beginning of his term in office, but only the former oligarchs were replaced by new oligarchs.

To prevent dissent from the current political system, a comprehensive surveillance and censorship program was initially launched against the country’s own population. The so-called “SORM” system was conceived during the time of President Yeltsin in 1994. However, it was at the beginning of the new millennium that SORM-2 was applied to the Internet. Providers were forced to install monitoring devices on their servers at

*“In mid-2017, Twitter introduced changes to their platform, making life harder for bots. Prior to this, detecting bots was often as easy as clicking on the top item in the list of trending hashtags in the Russian Federation, and any number of near identical accounts posting the exact same message could be found.”*

Dr. Rolf Fredheim, NATO StratCom COE

their own expense. These monitor and document all financial transactions, email messages, and user behavior on the web. Since 2014, the latest version of the technology SORM-3 also documents all social media channels, blocks encryption programs and is able to assign devices, data packets and all data transfers to a specific user with Deep Packet Inspection (DPI). The KGB no longer exists; its extensive competencies have been transferred to the FSB and SVR services. Here is a brief description of the exact capabilities currently maintained by each of the Russian Federation’s intelligence services.

**SVR** (Служба внешней разведки, Sluzhba vneshney razvedki – Foreign Intelligence Service)

The SVR reports directly to the President of the Russian Federation and works closely with military intelligence. It is also empowered to install agents abroad illegally through so-called “active defense” and has a large arsenal of technical capabilities.

Directorate I is the special department for computer-aided acquisition of intelligence information. It also analyzes and evaluates the material and makes it available for further use.

**GRU** (Главное разведывательное управление, Glavnoye Razvedyvatel’noye upravlyenie – Headquarters for reconnaissance)

The GRU is the military intelligence service of the Russian armed forces and officially no longer operates under that name, but since 2010 has been called the “Main Administration of the General Staff of the Armed Forces of the Russian Federation.” Although not even Vladimir Putin calls the service by its “new” name, there is much that is revealing in the designation. The GRU is virtually at the center of the armed forces and is not just an affiliated auxiliary structure.

#### ■ Unit 54777

This unit is engaged in “psychological warfare,” which includes placing targeted disinformation in states per-

ceived as “hostile” in order to “influence public opinion,” according to widespread notions. Another target group is the Russian-speaking diaspora abroad. Recently, it became known that the unit was probably also involved in the placement of misinformation concerning the coronavirus.

#### ■ Unit 26165

Also known as “Fancy Bear,” “Strontium,” and “APT 28” conducts cyberattacks on the digital infrastructure and resources of “hostile states” and seeks to achieve financial, structural, and technological damage. But also by exploiting vulnerabilities in security systems to place spectacular messages and threats to shake the sense of security. The unit has perfected the practice of “spearfishing,” “zero-day,” and malware (more on these topics in the “Cyber Attacks” chapter) in its hacking attacks.

#### ■ Unit 74455

Also known as “Sandworm” deals with the professionalized theft of information, as was evident in the course of the 2016 US-presidential election. But these are actually not the most spectacular attacks of this unit. It also deals with attacks on critical infrastructures of “enemy” states. For example, the attacks on the Ukrainian power grid in 2014, the NotPetya affair (a so called wiper worm, which deletes data without possibility to recover), or the attempted manipulation of the presidential election in France in 2017.

### The Internet Research Agency (IRA)

It conducts most of the operations, that is a para-state organization that is privately owned. It creates fake personas, instructs real persons and news agencies and creates structures that persist over a long time-span. The IRA is more successful than the **GRU**, which is the Russian intelligence service for international affairs. Speaking about propaganda and disinformation, the



Figure 11: Russian cognitive warfare makes use of the classic Conflict Triangle to intensify social polarization by means of Fake News, and Social Media disinformation campaigns. (NATO STANDARD AJP-01(F))

IRA regards narratives that are overlapping each other and are organized in a very repetitive way might prevail to accomplish a propaganda task. It is worth to mention, that this agency as well still follows the rulebook of *active measures*, the paradigm of Soviet and now Russian intelligence. While in the case of the Wikileaks involvement in the US elections 2016, it was traditional US media – and not social media – that started to be interested in the material, the data itself was delivered by Russian hackers.

### Russian disinformation – methods and what are the real goals

“In mid-2017, Twitter introduced changes to their platform, making life harder for bots. Prior to this, detecting bots was often as easy as clicking on the top item in the list of trending hashtags in the Russian Federation, and any number of near identical accounts posting the exact same message could be found.”

Popular opinion has it, that the intrusion by, allegedly and most likely, Russian hackers in Estonia in 2007 were the first comprehensive “cyber-attack” that has been documented. Back then unknown hackers most likely aligned to the pro-Russian youth organization “Nashi”<sup>18</sup> attacked websites of the Estonian government, national banks and media. This is seen as a reprisal for the removal of a Soviet era war memorial in the city center of the Estonian capital Tallinn. Notwithstanding the significance of this event, this perception is not entirely correct. Thus, the first large scale activity of that kind was the massive online spying by the National Security Agency (NSA) in the United States on

its own population from 2001 onwards (i.e. after the terrorist attacks on the US of 11 September 2001), as well as subsequently on governments and populations of allied countries, including Germany. These actions contributed a lot to the increasing efforts of powers like China and Russia, to strengthen their cyber capabilities, to counter the US, because they feared that they might get overpowered. In other words: there are manifold backlashes and unintended consequences of the “war on terror”.

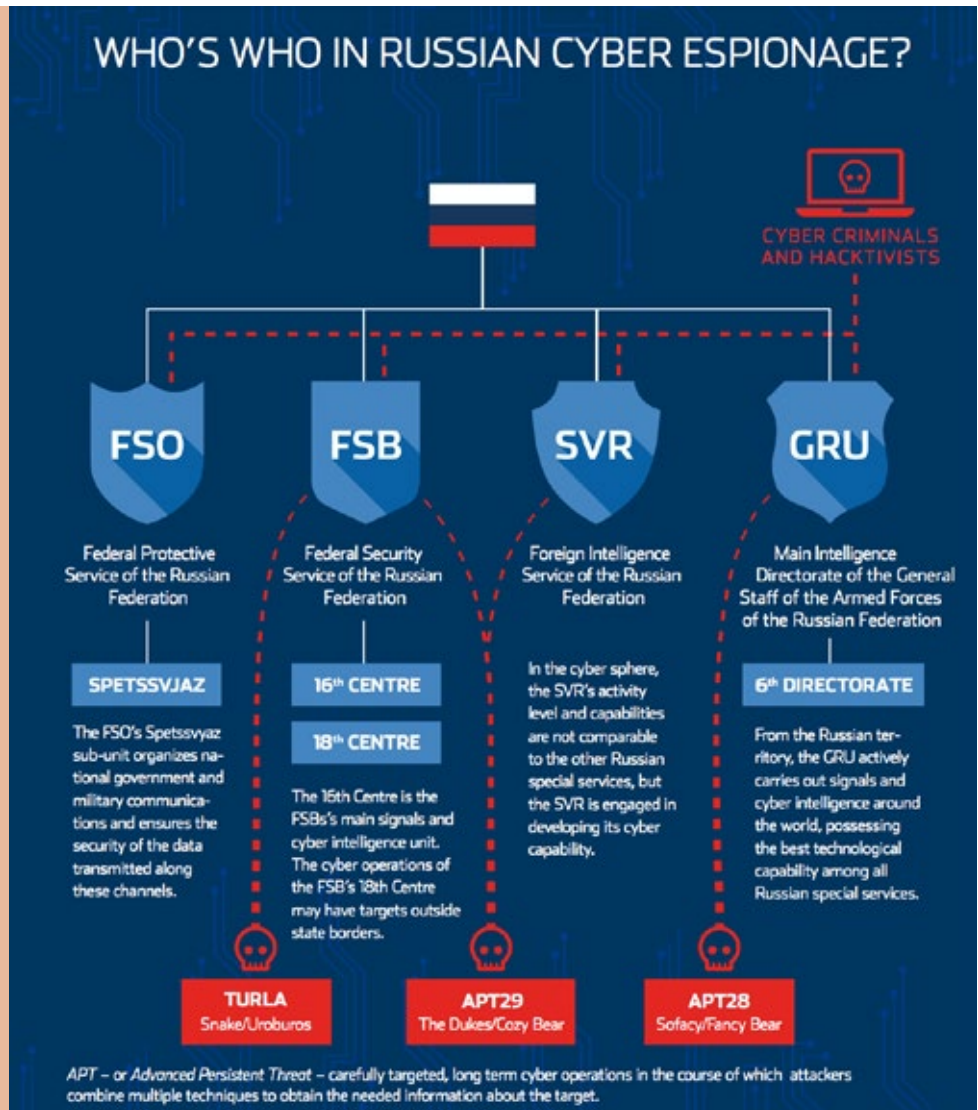
Online disinformation, and Russian disinformation is no exception, does not aim to create new patterns of opinion, but to deepen existing divisions within a society. The term “disinformation” is not entirely accurate in the case of the Russian strategy either. Rather, one must differentiate between different areas.

### Fields of activity

#### On the social networks

- Twitter: The main field of activity. Here Russian services massively use fake accounts, semi-automated programs (bots) and manipulated media content.
- Facebook: The secondary arena. Fake accounts and straw man groups are used to simulate discourse.
- Instagram: Another sideshow. Here, the comment columns of politicians critical of the regime are “spammed”, or accounts are created that are supposed to show Russian “heroes” in the fight in Ukraine.

Figure 12:  
The Russian cyber espionage and sabotage infrastructure. Courtesy of oodaloop.com



### Messenger Services

- This includes so-called “news groups” on the app Telegram or Whatsapp, for example. These have particularly increased their activity since the Russian attack on Ukraine.

### Own Russian Media Outlets for the International Audience

- State propaganda channels aimed at an international audience: These include RT (formerly Russia Today), Sputnik, and Ruptly, for example. These are currently more or less banned from broadcasting in the European Union.
- Fakes of existing news portals: Russian programmers have already repeatedly copied existing web-

sites of media portals (Bild, Spiegel, etc.) deceptively genuinely and filled them with fictitious content.

## Types of Russian Online Propaganda

### 1. Disinformation

News is spread whose content has never taken place. Information is disseminated that is untrue or does not fully reflect the truth. But it serves to polarize along social fault lines. To this end, the Internet Research Agency, for example, runs an entire department dedicated to analyzing socio-political developments in the target countries. Disinformation is very difficult to combat because, once spread, it has a higher and more resilient spread than counterstatements. The more



authentic the disinformation has been crafted and the more complex and diverse the “sources” of it are, the more difficult it is to expose.

At this point, it must be made clear that, contrary to popular media portrayal, Russian online disinformation is rarely direct and obvious lies. Rather, it follows the best tradition of successful propaganda – not being a complete lie, but not being the whole truth either. Truth with a certain twist, describes this circumstance quite well. False links are made, untrue context is used, etc.

### **2. Deep Fakes**

These are such perfectly faked images and video recordings that they can only be debunked with the help of sophisticated technology. In a narrower sense, this is also disinformation, but it does not require text and is therefore on a different sensory level than purely verbal messages. They can either appear as stand-alone propaganda and “speak for themselves”, so to speak, or serve as fictitious “evidence” to support a confabulated narrative.

Here are a few brief examples of how Russian Internet trolls, also called “Кремлеботы” (“Kremlboty,” “Kremlin bots”), have attempted to influence public debate on social networks in Germany or the United States, for example.

### **3. „Troll Farms“**

In 2015, former German Chancellor Angela Merkel joined the Instagram platform. It wasn’t long before her comments column was filled with countless messages in Russian. Among other things, it was said that she was in pact with “fascists” in Ukraine. This was probably the first test attempt of the Russian trolls, because very quickly there was an increase in spam attacks in German. The trolls either comment on existing postings of foreign media and persons, or they try to simulate an artificial audience for media offers originating from the Russian Federation itself.

According to statements by former employees of IRA subcompanies, entire departments are assigned, in some cases with a total strength of 400 people, who do nothing but spread invective comments and false news using fake accounts – hence the name „troll farms“.

### **4. Reinforcement of social friction lines through simulated discourses**

In 2017, a campaign on social media called “Blacktivist” managed to pass itself off as part of the Black Lives Matter (BLM) movement, but was actually run by Russian agitators. It even managed to generate more followers on Facebook and Twitter than the authentic BLM channels.

On “Blacktivist,” an attempt was made to further radicalize the African-American protest movement, or to portray BLM in the eyes of the white population as a group that desired a “race war” in the United States. In the process, fake Facebook and Twitter accounts communicated with each other, pretending to be authentic discussions between authentic people. With success, real users jumped on it.

But the campaign proved itself to be a fraud. The texts and calls were full of language features that would be unusual for a native English speaker and pointed to third-party control. Facebook and Twitter cooperated with U.S. authorities, who were able to trace the activities back to Russia, according to self-reporting.

### **5. „News Groups“ on Telegram**

In the wake of Russia’s attack on Ukraine on February 24, 2022, a large number of new, so-called “news groups” emerged on the messenger service Telegram. Primarily in the English language. These disseminate decidedly pro-Russian documentation of the events in Ukraine. Every day, countless short clips of fighting, Russian weapons systems and operations are posted there – but they can hardly be verified. In a smug tone of voice, losses of Ukrainian units are commented on there, but also own failures are played down, targeted fears in Europe are served (economic ruin of the EU, power cuts, nuclear war, etc.). Through “appeals for donations” it is pretended that the channels are run by individual “independent” users. However, it is noticeable that the postings on all channels are identical and their activity times fit into the Moscow time zone.

### **6. Cyber sabotage by Russian hackers**

In the course of Russia’s attack on Ukraine, but also beforehand, there were attempts by Russian hackers to actively damage the country’s critical infrastructure. This includes, for example, the state administration, the banking sector, the power supply and the internet coverage itself in the country.

*„First of all, some cyber-attacks were well prepared and executed in the beginning of the war, especially to stop information dissemination and to create confusion. To all appearances, Russia’s initial military strategy was based on a very short, fierce warfare and swift military success. Therefore, Russia had probably not planned cyber activities beyond those initially conducted. Due to the necessary extensive preparations for military cyber activities, it was not possible to increase these on short notice and consequently adapt to the changed war situation. Russia’s conventional armed forces have been reported to be heavily dependent on Ukrainian ICT infrastructures (e.g. combatants had to resort to their own private ICT devices). Non-state actors on both sides of the conflict have developed enormous and unexpected activities in cyberspace, supporting their respective side, which has probably also involved IT forces. We have even seen non-state vs. non-state actor hacking attacks and data breaches. The IT infrastructures in the Ukraine has been proven to be quite resilient. On the one hand, this is because it has a very decentralized structure. In addition, foreign IT forces have also helped with intelligence information in the run-up to and during the war.”*

Thomas Reinhold, research associate as well as PhD student at the Chair of Science and Technology for Peace and Security (PEASEC) at the Department of Computer Science, TU Darmstadt

- In 2015, an attack on an electricity supplier in western Ukraine cut off supply to more than 200,000 households. Using phishing emails (as in the China example) and Trojans, the hackers worked their way into the substation control centers. There, network sections were disconnected from each other and wipers prevented rapid restoration. This was the first attack of its kind on a critical infrastructure system.
- Back in January 2022, various Ukrainian government websites were attacked and blocked.
- In February 2022, malware (Trojan) infiltrated programs were activated on the servers of banks. So-called “wipers” (automated deletion programs) destroyed the databases of various institutions. This was already practiced by Moscow in the years before (NotPetya Affair). The malware Acid Rain specifically attacked Ukrainian servers right before the imminent assault of the Russian Army on the country and wiped modems in the region. As a result, Ukraine had problems with its overall access to the internet.
- Immediately before the attacks, the websites of Ukrainian ministries were again paralyzed and subjected to so-called “defacing”. In the process, a text in Russian, Ukrainian and Polish was loaded onto the home page, warning, among other things, that those who had been guilty of something should “be afraid and expect the worst”. This incident bears aspects of propaganda and hacking.

However, it must be noted at this point that the attacks were smaller than was assumed in 2014, at the beginning of the civil war in Ukraine. This is due to several factors.

It was not possible to paralyze the energy supply throughout the entire country, as the grids were also connected to the regions in the Donbass and Crimea that were already under Russian control. A large-scale blackout would possibly have had consequences for these areas as well.

Contrary to popular belief, hacker attacks were not able to directly influence events on the battlefield. Complex weapon systems are equipped with (mostly) autonomous systems that have a high degree of resilience against such attacks due to their decoupling. However, there have been incidents that have either affected the critical digital infrastructure or, through the use of the Internet itself, have influenced battles in individual cases.

- At the very beginning of the attack in February 2022, Russian forces destroyed server facilities in locations that were important for the Ukrainian government and the country’s armed forces. The location of these facilities had already been determined in advance through covert cyber reconnaissance. One consequence of this was the Ukrainian government’s request to provide equipment from the satellite communications company Starlink for compensation.
- The Russian Air Force’s airstrikes on energy supplies also put the Internet out of action in large parts of the country. This vividly illustrates the “double effect” of physical attacks on the power supply. The destruction of transformer stations, power plants and lines not only paralyzes street lighting, machinery and water pumps – it also cuts off all communication and connection with the outside world through the Internet.

Despite everything, it is striking that Russia has not exploited the full potential of its cyber warfare in its war in Ukraine. This may also be related to the fact that there may now be a similar balance of power in the area of “cyberweapons” between the U.S., Russia, China, and other actors as there already is in the area of nuclear weapons.

In 2009, reports leaked out that the U.S. electrical grid had been infiltrated by Russian services. Ten years later, in 2019, the Russian Federation accused the U.S. of also compromising its power grid in return.

This is where so-called zeroday exploits and logic bombs play a role. Hackers are often able to find vulnerabilities in systems without the manufacturers, or the users, themselves being aware of them. However, the respective saboteurs do not exploit these entry points immediately, but rather store their knowledge and possible malicious strategies for a day X. As soon as

the attack takes place, however, the operators have “zero days” to close this gateway, hence the name.

Logic bombs are malicious programs that are able to act autonomously when certain circumstances occur. This does not even require a special command from a hacker group. Nor does it have to be a complete program; it can just be a code sequence.

A scenario such as the one that occurred in Ukraine in 2015 with the attack on the power grid of western Ukraine can also be carried out on a larger scale – on the computers and servers of the control systems of power plants and substations, with catastrophic consequences.

In this regard, the military and intelligence bodies of the Russian Federation have proved several times in the past that they are capable of carrying out devastating attacks. Some spectacular attacks were carried out, which, although the responsibility was denied by the official side, should probably be understood as a demonstration and a warning shot.

- The Colonial Pipeline ransomware attacks in the US in 2021. A hacker group called DarkSide, believed to have originated in Eastern Europe, shut down a pipeline system in the southwestern US that transports fuel for cars, trucks and even planes. The ransomware, which is extortion software, only lifted the blockade after the company paid 75 bitcoin, about \$4.4 million U.S. at the time. During the blockade, chaotic conditions ensued. Hoarding purchases exacerbated fuel shortages in many regions. Attribution was unsuccessful, so it cannot be said with certainty that Kremlin-affiliated hackers were involved. However, the suspicion is reasonable.
- Killnet, a hacker group whose proximity to the Kremlin has been documented, has also been covering Western states with attempted hacking attacks in the context of so-called “patriotic hacking” since the start of the Russian invasion. This involves (ostensibly) private hacker groups attacking the infrastructure of the “enemy” on behalf of their state. Killnet attempted to cripple sites of the governments of Romania, Italy, the Czech Republic, Japan, the USA and other states with DDoS attacks.
- APT28, also known as “Fancy Bear”, was behind the spearfishing attacks on the mail folders of the election campaigns of French President Emmanuel Macron and U.S. presidential candidate Hillary Clin-

ton in 2016, on computers of the German Bundestag and individual members of parliament, on NATO servers through so-called “spoofing” (impersonating existing accounts) and an unprotected Android app developed by the Ukrainian army to control the fire of howitzers after the start of the invasion.

## Conclusions:

From these examples (online disinformation and cyber sabotage), it can be deduced that attacks by Russian hacker groups have always aimed to undermine the defense capability, stability, and resilience of a target state, or organization. This is sought by:

- Generating the greatest possible polarization and insecurity among the population through spectacular hacking attacks on civilian infrastructure and by spreading disinformation.
- Generating a loss of confidence among the population in the democratic, state organs and decision-makers of a target country
- Weakening of military defense capabilities through infiltration of networks, communication lines, data storage and technologies
- Possibility of a cyber first strike on a target country’s critical infrastructure

## The following steps are recommended in dealing with Russian online disinformation and cyber sabotage.

### Online Disinformation

#### On the state level

Online disinformation is a challenge that is not easy to master. As it turns out, most “fact checkers” also show deficits, as they in turn only illuminate information from a certain perspective, or commit glaring errors themselves (more on this in the section “Fact Checking Fallacies” in the following chapter). The misconception must be abandoned that online disinformation is simply lies. Rather, information should be soberly analyzed for the real core it represents, but for the deliberate misinterpretation, linkage, and contextualization by Russian propaganda units. To what extent the ban on media formats from the Russian Federation has led to a mystification of the same cannot be assessed at this time. Nevertheless, the ban can easily be circum-



“Don’t feed the trolls” this advice is still valid in the internet.

vented with a VPN and shows that pure bans in the online sphere easily reach their limits.

#### At the civil society level

Digital literacy is still in its infancy in the European Union. Content from the Internet is often consumed uncritically by the population. There is still a lack of healthy skepticism toward online content. However, this is also promoted by the fact that content is only briefly read on the Internet and that the flood of information has become gigantic. The eroding culture of debate is doing the rest: Users often only read content that underscores and reinforces their already existing opinions. What is needed here, especially in schools, is to continue to promote education in an active and fair culture of debate that takes all opinions into account.

### Cyber Sabotage

#### On the military level

Communications infrastructure must be more actively defended. This also includes building up appropriate

hackback capabilities as a deterrent. However, this also includes a serious ability to accurately attribute attacks. The diplomatic and geopolitical consequences of hacks and hackbacks can be extensive and can also lead to open warfare if they result in physical damage.

**At the civilian state level**

European Union and NATO nations must agree on a unified and centralized approach to reporting, analyzing, and preventing hacking attacks on critical infrastructure. This must be able to respond efficiently and quickly to threats. The individual states should commit themselves to actively search for security gaps in order to be able to prevent the exploitation of a Zeroday backdoor even before an attack.

**Sources and Further Readings:**

**Center for European Policy Analysis (CEPA):** Russian Cyberwarfare: Unpacking the Kremlin’s Capabilities. September 08, 2022. By Andrei Soldatov and Irina Borogan.



**RAND Corporation:** The Russian “Firehose of Falsehood” Propaganda Model. Why It Might Work and Options to Counter It. 2016. by Christopher Paul and Miriam Matthews.



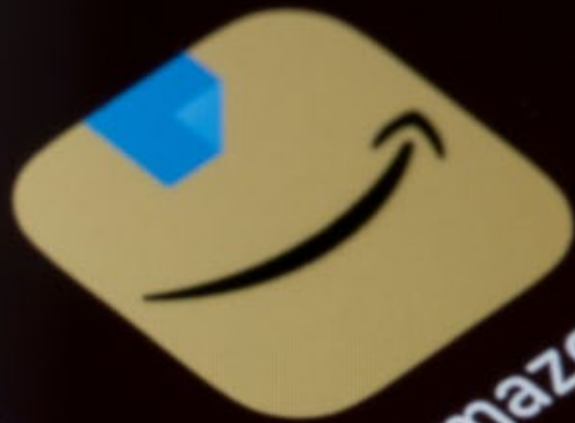
**CyberThreat.Report:** Analysis of the “#VulkanFiles” Leak. March 31, 2023. Katalin Béres.



**Zeitschrift für Friedens- und Konfliktforschung:** Regarding the debate on the containment of cyberwar: Analysis of military cyber activities in Russia’s war against Ukraine. 2023. By Thomas Reinhold and Christian Reuter.



# Big Tech



Amazon



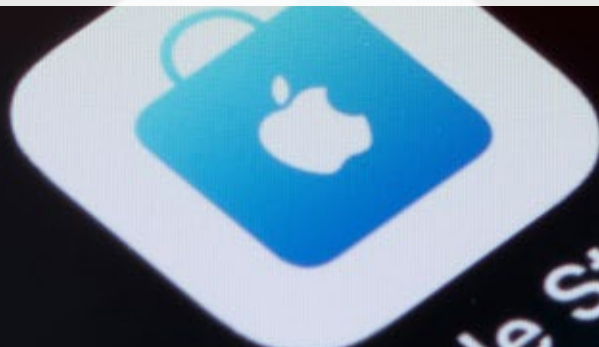
Facebook



Beautiful icons, lots of bright colors on the display. That's probably what most of us think the screen looks like. But the variety and the supposedly friendly interface are deceptive: Behind the apps are tough corporations that do business with our data, and accumulate profit.



Netflix



App Store



# 8 Big Tech – Obscure Friends

The aftermath of the so-called “Twitter leaks” received little attention in the German press, although they provided a unique insight into the internal workings of the social media group. Although Elon Musk can be viewed critically, his publications were more than revealing for understanding the role of multinational corporations in the area of “new technologies”: social media, search engines, and web applications.

At the same time, these publications have provided a new perspective on various issues that have arisen within the research of communication on social media.

1. does Twitter itself intervene in the communication flows?
2. is Twitter itself influenced?

Here, first, is the short answer to these two questions. Twitter intervened massively in the communication flows on the platform in several situations. This was done in part in cooperation with think tanks, other companies, government bodies, and reflected a certain political stance within Twitter itself.

Herein lies one of the most fundamental problems: Because platforms such as Twitter, Facebook, Instagram, and TikTok are corporate property of the respective companies, they can also determine what content is disseminated there and how it is disseminated. In contrast to the public perception, this is not a medium on which absolutely free expression of opinion can take place; this depends much more on the political attitude of the respective company management and is reflected in the preference for a certain spectrum of opinion.

The conventional wisdom is that the popular social media platforms are a free-for-all where the “marketplace of ideas” is best realized in a democratic fashion. This is not the case, however, and there needs to be a discussion about how the power structures that accumulate behind the corporate boardroom influence our democratic culture of debate.

## Opaque algorithm

Although many computer and social scientists are trying to understand the exact algorithm of Twitter, more specifically how messages are distributed and presented, to date much of this is still conjecture. No one knows exactly how these processes take place, and the company has also remained silent to this day, despite the takeover by Elon Musk and his promise of transparency.

However, there are questionable implications for free democratic expression here, which cannot simply be dismissed out of hand with the owner’s domiciliary rights. Millions of users communicate with each other on Twitter. As of 2023, Twitter has around 450 million monthly active users, and this number is estimated to reach 652.23 million by 2028<sup>19</sup>. Even if only a fraction of society in Germany and the EU uses this platform despite the media’s portrayal of it, it is still a medium on which opinions are produced and multiplied. This makes the Twitter communication system particularly susceptible to intervention by those who operate it and thus have absolute dominance of the discourse there.

## COVID on Twitter: how renowned experts were defamed as quacks

Despite all protestations, Twitter not only filtered out obvious disinformation campaigns from the discussion. But also the voices of established scientists, recognized members of the academic public, who, however, were not supposed to have their say due to the political perception of the responsible censors on the platform.

The goal was to combat apparent “disinformation” on the platform about COVID-19. It was an important concern, for both the Trump and Biden administrations, to combat misleading information. After all, many

anti-vaxxers and other conspiracy myths had proliferated on Twitter. It quickly overshoot the mark drastically, however, and so people who are clearly renowned scientists were also excluded from the discourse simply because they did not toe the increasingly narrow official government line. For example, University of Oxford professor Carl Heneghan was banned from Twitter for posting an article that was critical of the UK government's handling of the pandemic<sup>20</sup>.

Another good example is Harvard epidemiologist Martin Kulldorff, whose analyses produced results that were critical of the CDC's strategy in the United States<sup>21</sup>. His case, however, is only one of many. However, this debate was apparently not desired and so both the Trump and Biden administrations intervened with the management of Twitter to prevent this.

In the Kulldorff example, leaked internal messages exchanged between Twitter employees show that he was to be branded a "source of disinformation" – which is what happened. How was this possible? After all, he's not some corona denier, or anti-vaxxer.

The reason lay in the fact that the entire staff at Twitter tasked with reviewing content had no medical training whatsoever. Nor were they trained to distinguish scientific debate from propaganda. The team focused solely on recognizing the CDC's report on the coronavirus as truth and developed increasingly rigid exclusionary mechanisms.

The work of the legal, policy, and trust department at Twitter took on such proportions that it seemed necessary to even move the work to an outsourcing program in the Philippines. Employees without any medical or scientific expertise were required to report tweets and accounts based on "decision trees". These had been created in advance to "facilitate" the work, since they no longer had to deal with background information.

In the end, in the best case, disclaimers were added accusing the authors of "misleading". For the most part, however, a whole series of renowned and reputable scientists were blacklisted: Their tweets were restricted in their reach, their hashtags were ranked very low on the popularity scale, and even their own followers saw only partial news from them.

So the shadowban took hold again.

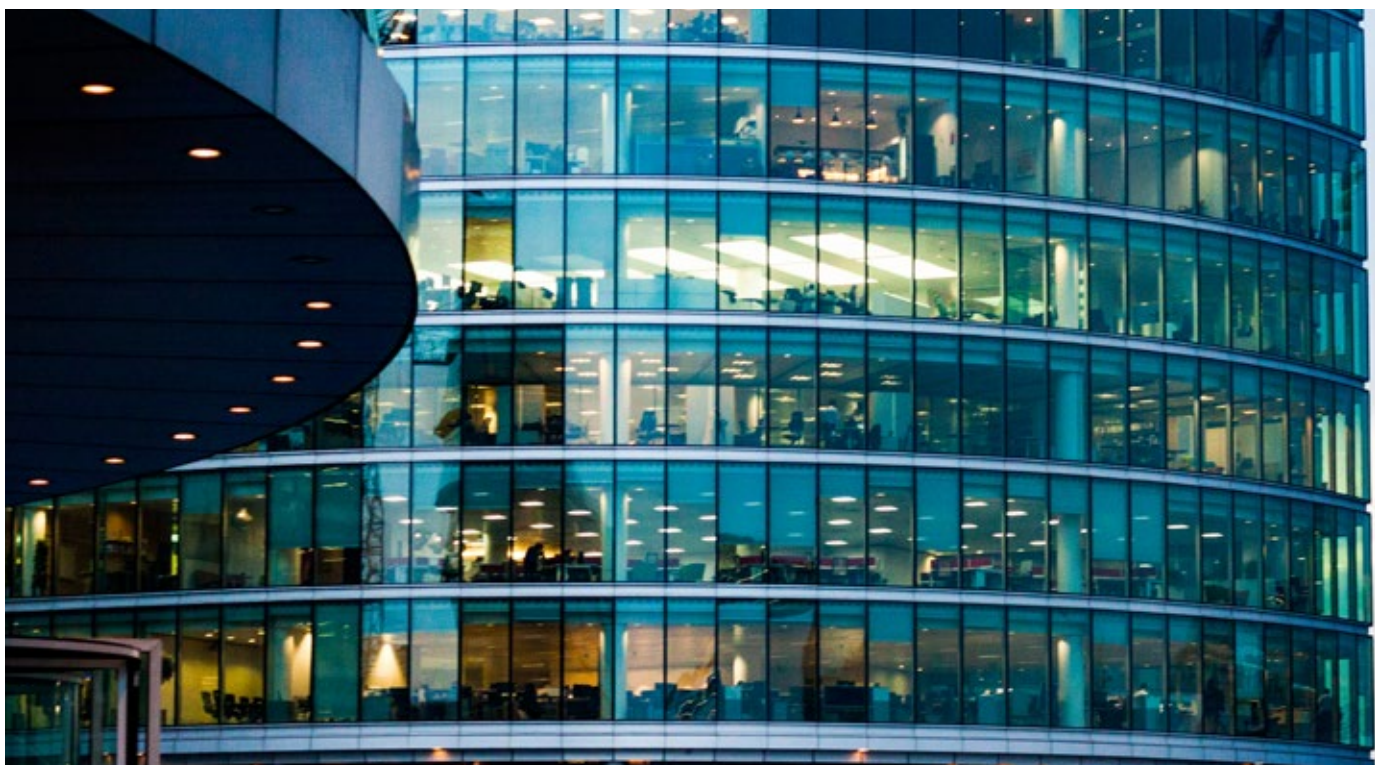
**Shadowban**, also called comment ghosting, refers to the throttling of the reach of a single, actively producing account by the platform operator without the user's knowledge. The ban can only be detected indirectly. For example, by analyzing the change in follower behavior, i.e., those accounts that follow the content of the banned person and interact with him or her. Twitter developed a complex system for this, called "Visibility Filtering". This put terms on an index and blacklisted accounts that used them. The interactivity of the tweets of these accounts was throttled in such a way that no one except the creator saw them. This kind of opinion control is not limited to Twitter. It is also widespread on YouTube, Facebook and TikTok. All platforms have denied this method of operation, except for one: YouTube. There, they even resorted to the drastic means of de-monetizing disagreeable opinions. Roughly speaking, money can theoretically be made with accounts that have more than 100,000 followers. In the case of "disinformation," however suspected, some content creators were deprived of their source of income – YouTube simply cut off their cash flow.

## There are still "equals" below the equals

The intention here is not to advertise a particular political orientation, but rather to show how certain Twitter policies lead to influential political cartels wanting to manipulate and censor public debate. This refers to the Democrats and the Republicans in the United States. They should be called cartels at this point because they are not just pure parties in the true sense of the word. They have an extensive network of capital-rich donors, such as large corporations, and they also have their own think tanks and PR organizations that intervene powerfully in the social debate. In no place has this been more evident than Twitter. The frightening thing is that neither political player has given itself anything in the process.

In 2016, the Republicans took unfair advantage of the leaked e-mail correspondences of candidate Hillary Clinton, and some members of the party even called on the Russian hackers to commit further such crimes.





One of the many symbols of the power of modern, international corporations: glazed high-rise facades.

The goal was not to facilitate constructive debate on substantive issues. It was much more about politically motivated defamation aimed at damaging the reputation of the political opponent. However, Twitter did nothing at the time.

However, the Democrats used their political influence on Twitter, coupled with the political orientation of the employees there themselves, to intervene in the debate in a steering manner. A good example of this is a 2020 New York Post article about files found on the laptop of Hunter Biden, the son of the sitting U.S. president. The Biden administration intervened in the strongest terms on Twitter. Since the Democrats had good connections up to the management of the social media platform, not only the accounts of the journalists who reported on the leaks, but also the main account of the New York Post were blocked and even the mere mention of this topic by anyone was censored.

But that's not all, the "Twitterfiles" also made clear how so-called "fact checkers" themselves synchronized their own political bias in interaction with the policy department of the big tech company. For example, many accounts of conservative users were falsely labeled as "Russian bots" and their reach was restricted, i.e. subjected to a shadowban.

## The case of TikTok

The application TikTok, or Douyin as it is also known in China, is a social short video platform operated by the company ByteDance, which is also based in the People's Republic.

The service, which allows users to upload short clips themselves and interact with others, has recently come under increased criticism – particularly in Europe and the United States. There are suspicions that the leadership in Beijing could spy on devices belonging to Western government employees if the app is installed on official phones. As a result, a full ban has already been mooted in the U.S., as it is also feared that China will try to target the General Population through propaganda.

In Europe, the Czech Republic is an example of a country that has already completely banned the use of the app for government employees.

*“Seeing it this way, the struggle against online disinformation should include raising awareness among journalists (and possibly also political actors) regarding the missing validity of social media data for representing public opinion. If they stop treating social media trends as ‘authentic’ expressions of public opinion, and hence stop amplifying these trends in their coverage, then a lot has already been gained in the struggle against online disinformation.”*

Prof. Dr. Florian Muhle, Chair of Communication Studies with a focus on digital communication, Zeppelin University Friedrichshafen

## Big tech can put our democracy at risk

As has been said, the point here is not to write for a particular political direction, it is much more to point out that questionable trends are emerging for liberal democracy.

Regardless of which side the shadowbans, blocking and censorship are with, it is in principle an unfair intrusion into the democratic culture of discourse. It should not be allowed to make a difference whether a user’s political opinion fits into a moderator’s world view or not – as long as it does not become criminally relevant. The problems of the social media and Internet technology giants amount to the following points:

### 1. The power of the algorithm

An algorithm for controlling a social media platform may be as sophisticated and complicated as it likes. Still, in many cases, it cannot replace human, expert judgment. It is unaware of the subtleties of the difference between satire, freedom of speech and dangerous hate speech. On the other hand, the mass of daily tweets would also overload the individual moderators, which is why decision trees are set up to help (which in principle are again nothing more than algorithms). A balanced system is not yet apparent.

### 2. Private ownership vs. socio-political responsibility

It is a question of state theory and law to what extent the right to private ownership and the socio-political responsibility of companies are weighted. Of course, Twitter is a company and therefore has the right to

determine what happens on the platform – and what does not. However, if a fundamental good, such as the right to freedom of expression and (at least in Germany) also a right to information free of censorship, is in danger, this weighting looks somewhat different. Of course, not all Germans use Twitter, but it is still an important multiplier of opinions and information that should not simply be allowed to invoke a domiciliary right.

This also becomes clear in the case of Elon Musk. Of course, the released Twitterfiles were a unique opportunity to look behind the scenes of the tech giant. Information that would probably never have been accessible was now openly accessible – and only because a single person felt politically impelled to do so. This is precisely the problem, because there are also problematic developments under Musk. His arbitrariness, for example, and the fact that the exact algorithm according to which Twitter works is still a company secret. This brings us to the next point.

### 3. Non-transparent structures

In contrast to state institutions, all social media and Internet big tech companies are extremely non-transparent about their business practices and exact internal workings. Likewise, the code in which the individual platforms are programmed is largely unknown. Until the release of the Twitterfiles, there was simply no knowledge of what internal actions are planned at Twitter, for example, how it is carried out, and what the implications are.

Social scientists, programmers and software analysts are literally poking around in a haystack to at least get some inkling about the internal mechanisms by which

*“Our conceptualizations of cyber warfare have, for too long, failed to fully incorporate and appreciate the ways in which domestic applications of cyber tools affect human security. Although domestic applications of states’ cyber capabilities are not new, much of the discourse around the dynamics and risks of cyber operations has focused on the interstate context.”*

Prof. Dr. Anita Gohdes, Professor of International and Cyber Security at the Hertie School



the platforms operate. Most of it remains speculation, and Musk’s publications will not change that. What remains astonishing, however, is that everything that was dismissed as “conspiracy theory” by the Twitter management before him actually proved true. This is a fact that must be faced.

Twitter is not alone in these alarming developments. As the world’s largest search engine, Google has the power to censor individual search terms and manipulate the results. In doing so, the company is naturally guided by the political guidelines of the respective countries, among other things, for very sober economic reasons. If you search for certain terms in the People’s Republic of China, you will sometimes get different results than a user in Germany would.

As can easily be seen in the Musk case, this possibility also creates an enormous problem. Not so much with himself, but with a functional circumstance. Should the heads of hierarchical structures, such as multinational corporations, be people who project questionable social experiments, our democracy will have a problem. Multinational corporations, which are also called the most effective expression of the strictest and perfect hierarchies, are independent of national borders, are not subject to democratic co-determination and are constantly trying to grow economically.

When this kind of purely economic power structure now enters directly into the field of political opinion-forming and sociopolitical discourse, a process

that would have been difficult to imagine 30 years ago, a lopsided situation arises. Social media played a role in democratic uprisings and protests in many countries from Serbia to the Middle East and Hong Kong – but can also work reversely, against democracies. So should Big Tech decide, hypothetically, to reject liberal democracy, it cannot be ruled out that they would be able to do enormous damage to our form of society.

This is best illustrated by a somewhat more pointed case: TikTok. If there has already been an ideological bias on Twitter, it is within the realm of probability that this platform will also be the site of events that have a clearly political thrust. TikTok is owned by a Chinese corporation and it cannot be ruled out that the platform is used for disinformation purposes or cyber espionage.

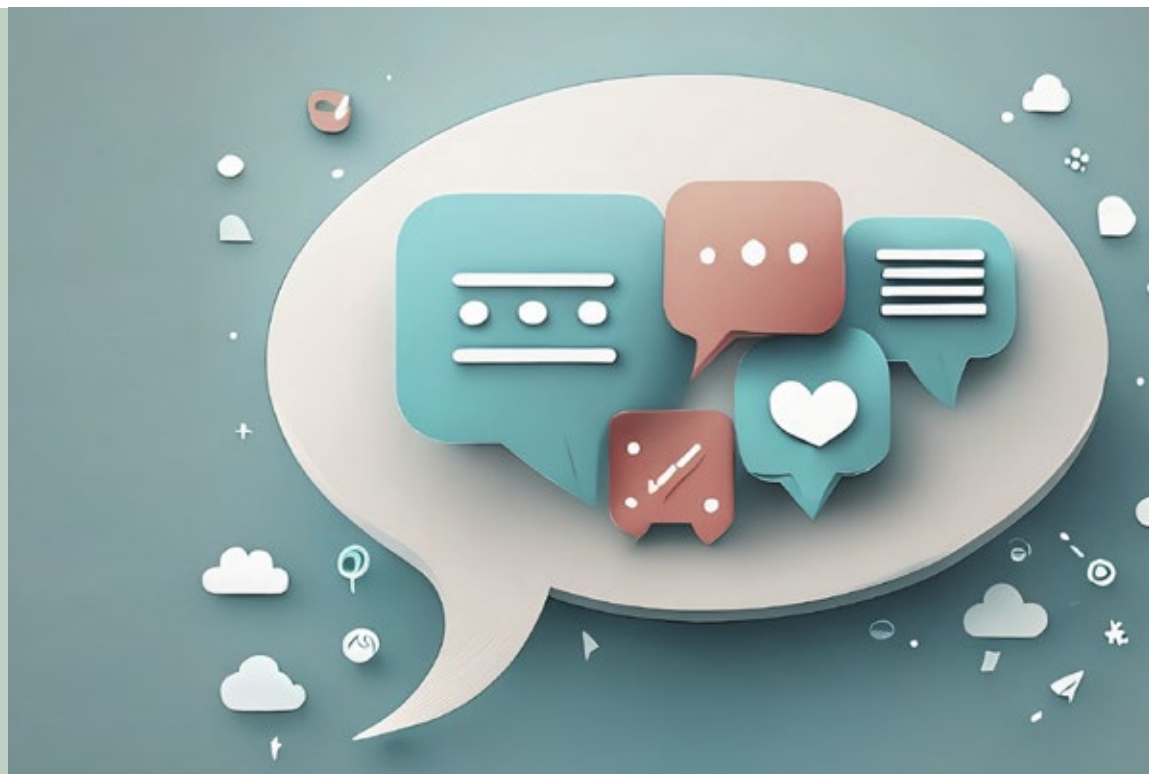
For this reason, there has been a debate in the USA since the beginning of 2023 to block TikTok completely. The Czech Republic has already instructed its civil servants not to use the platform on any official devices. The risk for security breaches is too great, it said.

The European Union, but also national governments, such as the one in Germany, have not yet fully understood the seriousness of the situation in this regard. The problem is seen more in the mass of users and the lack of a clear-name obligation. Of course, this is also an important area, but we will discuss it in the next chapter.

**Policy Recommendations:**

- It is bad policy to enable Big Tech companies to develop technologies that could be used to create technical structures that could easily be used as in a police state. Further it is bad policy to create legislation, that sides with those companies in creating such conditions without any checks and balances.
- Platforms like Twitter are also not comparable to newspapers, where it is clear that it is a one-speaks-to-many format. They are much more forums on which everyone should be able to communicate with each other on the same level (at least this is the basic idea). So here, a public good is directly touched, so to speak. A unique situation in which technology and immaterial democratic action and law meet directly. Too little account is taken of this fact.
- Special laws must be drafted to ensure more solutions on the part of the big tech companies, not to impair indispensable, intangible goods of democracy. Freedom of expression and the right to uncensored information must not be made dependent on the personal, political views of a supervisory board member or a managing director.
- Big tech companies must be encouraged to develop transparent business practices and to fully inform the public about the precise functioning of their platforms.

Even though everything is in bright colors, most of the content on social media is frequently rather black and white.



## Sources and Further Readings:

### Shadowban

**Washington Post:** Shadowbanning is real: Here's how you end up muted by social media. December 27, 2022. By Geoffrey A. Fowler.



**Neue Zürcher Zeitung (NZZ):** Donald Trump wird gesperrt, Ayatollah Khamenei darf weiter twittern – beim Kurznachrichtendienst herrscht politische Willkür. (In German: Donald Trump is blocked, Ayatollah Khamenei is allowed to continue tweeting – political arbitrariness reigns on the short message service). December 16, 2022. By Lucien Scherrer.



### Hunter Bidens Laptop, the New York Post and how bizarre Big Tech censorship has become

**The Atlantic:** Why Hunter Biden's Laptop Will Never Go Away. April 28, 2022. By Kaitlyn Tiffany.



### Big Tech endangering democracy

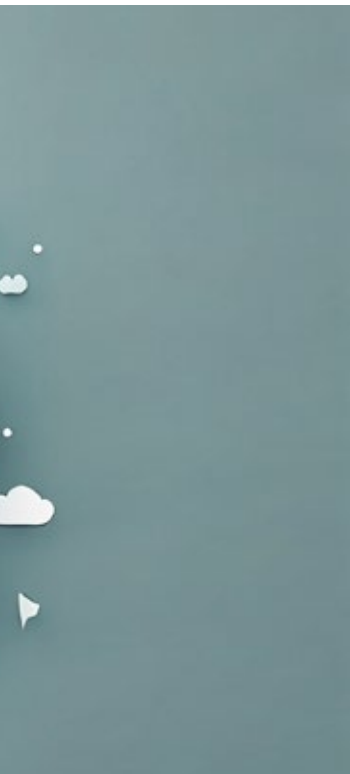
**United States House Committee on Oversight and Accountability:** The Cover Up: Big Tech, the Swamp, and Mainstream Media Coordinated to Censor Americans' Free Speech. February 08, 2023.



**Foreign Affairs:** How to Save Democracy From Technology. Ending Big Tech's Information Monopoly. November 24, 2020. By Francis Fukuyama, Barak Richman, and Ashish Goel.



**MIT Technology Review:** How Google took on China—and lost. December 19, 2018. By Matt Sheehan.



In a democracy, the rules of social coexistence must be negotiated with all those involved. So much for the theory, but as circumstances become increasingly complex, this becomes more and more complicated. This section will focus on the current state of affairs in the areas of democracy and cyber security, defense and civil liberty.



## 9 STATE of PLAY: How do Germany, the EU, NATO and global initiatives aim to challenge international online disinformation and cyber insecurities

---

Every action naturally generates a counteraction, this law is also applicable to cyberspace. The EU, its member states and also NATO are responding to the emerging, increasingly massive challenge from global actors such as China, or Russia, but also from non-state actors such as multinational companies, organizations with potentially dangerous political agendas, with safeguards.

These include certification for software products, protection against malicious hacking and cyber extortion, cyber espionage, but also measures to combat disinformation and fake.

The main burden of attacks on the territory of the European Union lies on the Public Administration and Digital Service Providers. This means that government institutions are in the crosshairs and these are direct attacks on the functioning of nations. However, attacks on Digital Service Providers are also direct threats to

the functionality of state, economic and scientific structures.

Threats of this kind are present at all levels, because what affects the EU also affects its member states. It is the same with NATO: threats to its military security also affect the individual alliance countries.

Therein lies the duplicity of the relationships of supranational structures and their individual states within the complex of cybersecurity and online disinformation: the sum total of the related problems of the individual states are automatically also threats to the supranational structure and vice versa (and the same can be said about alliances like NATO).

Here, in sequence, the individual current efforts, legislative projects, reform efforts and initiatives currently started by the EU, NATO and Germany will be presented.

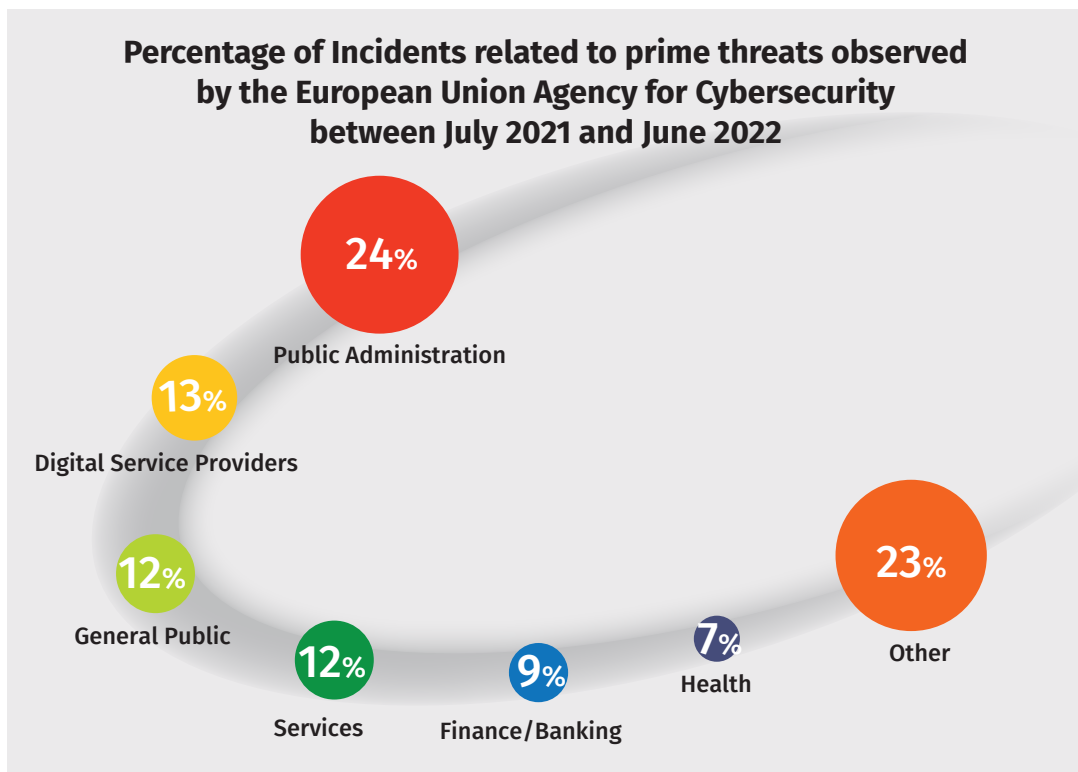


Figure 13: Public administration as the most frequent victim of cyber attacks may come as a surprise. Nevertheless, it is a lucrative target: this is where citizens' personal data can be obtained, which can later be misused by hackers. Source: Inhouse. Data: ENISA

## 1. THE EUROPEAN UNION

EU cyber legislation includes the Directive on attacks against information systems, the Network-Information-System Directive (NIS, currently in the revised new NIS2) and the EU Cybersecurity Act. Meanwhile, the EU strategy for data in Europe is built on four pillars: data protection, fundamental rights, cybersecurity, and safety.

In order to exactly understand, about what the EU is talking and what she understands as being a certain concept, we should first have a look on their basic definitions:

- Security of network and information systems: ability to resist actions that compromise data availability, authenticity, integrity or confidentiality.
- Cybersecurity: ensuring availability, authenticity, integrity and confidentiality of network and information systems and related services.
- Incident handling: actions aimed at detecting, analyzing, containing, and responding to incidents.
- Cyber threats: weakness, susceptibility or flaw in an asset, system, process, or control that can be exploited by a cyber threat.

- Examples of service providers: DNS (Domain Name System), top-level domain name registry, cloud computing, data center, content delivery network.

The EU's planned New Cybersecurity Strategy aims to focus on the following:

- Resilience, technological sovereignty and leadership
- Building operational capacity to prevent, deter and respond
- Advancing a global and open cyberspace through increased cooperation

In healthcare, energy, and transport, NIS 2 aims to boost cybersecurity and bolster digital resilience. This involves AI-driven Security Operations Centers, SME support via Digital Innovation Hubs, workforce upskilling, attracting global cybersecurity talent, and investing in research.

In addition to forming a Joint Cyber Unit, strengthening the EU Cyber Diplomacy Toolbox, and improving cyber defense through initiatives such as the European Defense Agency and Permanent Structured Cooperation, the European Union is forming a Joint Cyber Unit. EU engagement at the UN and other forums advocates for rules-based cyber security, human rights online,



## STATE OF PLAY

and international norms. EU cyber diplomacy will be built in third countries, dialogue intensified, and cyber capacity built.

Funding will be established at both the EU and member state levels for these ambitious initiatives. It will allocate financial support from:

Union level:

### Digital Europe Budget

A €7.5 billion initiative designed to expedite Europe's recovery and digital transformation. It prioritizes supercomputing, artificial intelligence, cybersecurity, advanced digital skills, and widespread adoption of digital technologies. The program bridges the gap between research and implementation, benefiting citizens, businesses, and small and medium-sized enterprises<sup>22</sup>.

### Horizon Europe

€95.5 billion (current prices) will be allocated for 2021–2027, including €5.4 billion from NextGenerationEU to drive recovery and enhance EU resilience, plus €4.5 billion in additional reinforcement. Horizon Europe is the world's most ambitious research and innovation programme, with a 30% increase (in constant prices) over Horizon 2020<sup>23</sup>.

**Digital Service Providers** is the collective term for all service providers that provide online infrastructure for web users. This includes cloud services, hosting and software development. The definition in the European NIS (Network Information Systems) Regulation reads: Article 4 (19) of the NIS Directive defines cloud computing service as meaning “a digital service that enables access to a scalable and elastic pool of shareable computing resources”. Any company that offers any of the three services would fall under this area:

‘Infrastructure as a Service (IaaS) – Third party hosting of hardware, software, storage, servers and other infrastructure for its users.

‘Platform as a Service’ (PaaS) – Provides a platform for users to develop, run and manage applications on the providers cloud service.

‘Software as a Service’ (SaaS) – A software distribution model where a cloud service provider hosts applications and makes them available to customers over the internet (typically accessed using a thin client via a web browser)



Figure 14: Various cyber strategies and their categories. Courtesy of cybersecurityforme.com

### Recovery Plan for Europe

After the COVID-19 pandemic, the EU's long-term budget and NextGenerationEU (NGEU), a temporary recovery measure, represent an unprecedented stimulus package of €2.018 trillion. This funding aims to make Europe more sustainable, digitally advanced, and resilient. Aside from providing emergency assistance and support in Ukraine and EU member states in the aftermath of Russian aggression, the funds are also used to mitigate humanitarian disasters<sup>24</sup>.

### Member state level:

#### EU Recovery and Resilience Facility

As a temporary recovery tool, the Facility allows the Commission to raise funds to support Member States in implementing reforms and investments aligned with EU priorities and addressing challenges identified under the European Semester framework. Loans and grants worth €723.8 billion are provided to achieve the EU's climate neutrality goal and promote digital transition, which will create jobs and growth<sup>25</sup>.

This is the framework of strategies and funding, but how does this look like on the operational level? In terms of policy and legislation, there are several very ambitious initiatives, reforms and plans.

#### Groundbreaking work: the Network-Information-Systems Directive (NIS) in its new form NIS2

In 2016, the original NIS legislation, developed since 2005, led to fragmentation within the EU's internal market. It was recognized by 2021 that it needed to be revised due to the vast changes in the digital landscape.

In light of evolving circumstances, the original NIS was deemed ineffective and inadequate. The NIS 2 directive proposal aims to enhance cyber resilience for EU businesses and address cybersecurity within the ICT supply chain. Across Member States, it harmonizes security and incident reporting requirements, national supervision, and enforcement. The new rules also increase cooperation among Member States through the NIS Group to prevent, handle, and respond to cybersecurity incidents. First of all, the directive reorganizes various legal and structural regulations:

The Resilience of Critical Entities (CER) Directive now covers 10 sectors (of former 5), including energy, transport, banking, health, and digital infrastructure.

**I**CT (Information-Communication-Technology) refers to any product or technology that deals with the storage, retrieval, manipulation, transmission, or reception of digital data. This includes products such as personal computers, digital televisions, email, and robots, among others. Essentially, ICT encompasses any technology that facilitates the processing of digital information.

- The DORA proposal seeks to standardize operational resilience and cybersecurity rules, reducing the need for individual Member States to establish their own standards and expectations.
- ENISA's mandate would be expanded to include preparing a biennial report on EU cybersecurity, maintaining a vulnerability registry, and creating a registry for specific entities.
- Coordinated risk assessments by the NIS Cooperation Group, the Commission and ENISA per sector to identify threats and vulnerabilities.
- The proposed directive would replace the security provisions of the European Electronic Communications Code (EECC) and regulate the security of all telecoms providers in the EU.

On an operational level, NIS2 is directed at mainly one major type of software, ICT (Information-Communication-Technology) and two different groups of entities in cyberspace: operators of essential services (OES, critical infrastructure, healthcare and digital infrastructure) and relevant digital service providers (RDSPs: online search engines, online marketplaces and cloud computing services). Systems in use must have sufficient security safeguards to protect data stored on devices, as well as services run by those operators. They are required to establish mechanisms for detecting vulnerabilities in their systems and to disclose any such vulnerabilities to responsible EU bodies (such as ENISA). To maintain protection, OES and RDSP must choose a reliable MSSP (Managed Security Service Provider). Moreover, constant exchange with academic and research institutions is emphasized to ensure continuous progress.

NIS2 requires Member States to adopt a national cybersecurity strategy, designate competent authorities, and establish CSIRTs (Computer Emergency Response

Teams) and promote information sharing. CSIR Teams will be in constant communication with ENISA, which will establish a vulnerability registry for defining flaws and backdoors.

However, EU CyCLONe (European Cyber Crises Liaison Organisation Network) and other cooperation groups will cover the horizontal dimension, that is, establishing and promoting trust among the various national CSIRTs. Also, this body will develop a coordinated response to cyber threats in due time, i.e. within 24 hours of an incident.

To establish transparency on who is hosting a website and running content or business with it, Domain Name Registrations and Domain Name Registers should be made public. Obviously, this only applies to people in the EU. Providers of DNS, TLD name registries, content delivery networks, cloud computing, data centers, and digital services that are not based in the Union will be required to choose a legal representative within the EU, fitted with a mandate to represent them. Reporting cyber incidents is explicitly included.

To better defend against cyber threats, the EU encourages knowledge sharing. It is necessary to process personal data for network and information security purposes, including raising awareness of specific cyber threats. The NIS2 claims, however, that the collection of data for security procedures must only be used for that purpose, for example, IP address of devices not directly involved in an incident will not be documented. The NIS2 directive provides sanctions and restrictions for those who do not comply with the directive's provisions in order to ensure compliance. These include monetary fines as well as revocation of licenses.

## EU Cyber Resilience Act

This act mainly concentrates on devices of the Internet of Things (IoT), which are in the EU lawmaking vocabulary called “products with digital elements”. Despite the fact that cybersecurity attacks targeting hardware and software products are causing considerable societal and economic costs, a majority of these products in the EU are currently not governed by any EU legislation specifically addressing their cybersecurity.

Five pillars of cyber resilience will be addressed by the EU CRA:

### ■ Prepare/Identify

Identification of possible threats beforehand and preparation of possible countermeasures

### ■ Protect

Improving the security of already existing devices, software and networks

### ■ Detect

Detecting of ongoing attempts to compromise the cybersecurity within the EU

### ■ Respond

Countermeasures against attacks from the cyberspace

### ■ Recover

Rectifying of damages that were caused by intrusions and assaults in the internet

The crossborder, that is in fact borderless, nature of events in cyberspace requires regulations that replace ineffective national measures. The proposed Regulation aims to standardize the regulatory framework in the EU and provide operators with more legal clarity by introducing cybersecurity requirements.

The identified problems and formulated objectives are sought to be more effectively addressed by adopting a regulation rather than a directive, as it would provide greater regulatory intervention.

As the CRA developed, the Commission consulted national market surveillance authorities, cybersecurity bodies, manufacturers, consumer organizations, and citizens.

Currently it a holistic approach is preferred by the EU Commission which is likely to be put in action: In it a regulatory intervention is suggested with cybersecurity requirements for both tangible and non-tangible products with digital elements, including non-embedded software, with two sub-options depending on the criticality of the software. It would avoid inconsistent security regulations for digital products, reduce the expenses of complying with cybersecurity laws, and enhance the reputation of companies globally, resulting in higher sales and demand for products with digital elements beyond the EU.

In very concrete steps this approach would look like this:

■ Identification and assessment of critical products and its classification into two classes of cybersecurity risk level

■ Developing of cybersecurity certificates by the EU Commission for the categorized products which each company has to obtain in order to make sales in the EU

■ Due diligence: manufacturers have to actively bear in mind to build in cybersecurity systems in their products, have to be transparent about it, and to hand their product over for assessment

- Unfinished software products can be made available and developers should not be prevented from doing so, but this should only be possible for a short period of time in order to test it
- The ultimate responsibility to observe and control the adherence to this regulations lies within the hands of the member states.

It is important to mention here, that a commentary provided by the European Parliament on these ideas forwarded as well the integration of a focus on Artificial Intelligence (AI) and products that use such in its operation. The New EU AI Act should in all fields in which AI is used override the provisions made in the EU Cyber Resilience Act in order to address the special high risk that could emerge from such systems. The assessment and analysis of the supplied product data by the developers will be conducted by ENISA.

For products, which are divided in the Annex of the proposal to the act into two classes (software and hardware) they must fulfill the following requirements:

- Absence of any known exploitable vulnerabilities (backdoors)
- Easy to reset
- Protection from unauthorized access
- Confidential storage of data, personal or other, protecting as well its integrity
- Usage of only relevant and necessary data for its operation (no data farming)
- Safeguard from manipulation and unauthorized remote control
- Possible sources of insecurity can be met with updates (cure and remedy)

## The EU Artificial Intelligence Act (AI Act)

The European Parliament has adopted several resolutions on artificial intelligence, covering topics such as ethics, liability, copyright, criminal matters, education, culture, and audiovisual. The Parliament suggests legislative measures to leverage AI's potential benefits while protecting ethical principles in these resolutions. The European commission defines as Artificial Intelligence software and devices with the following features:

**(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;**

**(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive**

## AI – rapid development with an open end

Artificial intelligence is currently the focus of media debate and public interest. Due to its diametrically opposed points of view, the discussion contains paradoxes. On the one hand, AI is hailed as a potential savior for humans, while on the other hand, extreme risks are cited, such as the disenfranchisement of humans, and the rise of machines that rule humanity. In a Reuters/Ipsos poll, 61% of Americans said that the growth of artificial intelligence technology could put the future of humanity at risk<sup>26</sup>.

Several decades ago, similar patterns were also seen in the debate about robots automating work. However, this is also the reason why this compendium does not focus more strongly on this new technology. Developments are too fresh and too difficult to analyze to produce a scientifically assured picture that could meet the standards of this work. What is certain, however, is that AI represents an absolute novelty that has the potential to permanently change our society, politics and economy; it is virtually a “third digital revolution.” For instance, AI-driven automation can cause large-scale job losses, which could lead to increased inequality across the world, and a need for more retraining of personnel<sup>27</sup>. This picture emerges if we assume the first as the establishment of the Internet as a mass communication medium and as the second revolution the emergence of IoT devices and related human interaction concepts.

Administrative acts can be facilitated by the use of AI, information offers from the government side can be provided faster and more personalized, as well as services by companies. AI facilitates literature research and text processing, as well as the analysis of information. These are only a few of the positive possibilities of the application of AI.

On the other hand, there is of course also a risk potential, which has so far only been suspected to a large extent<sup>28</sup>. Here, of course, the media work with very blatantly exaggerated scenarios and really dangerous possibilities are not ana-

*“If we do not get in front of current technological development; if we do not think ahead about its potential use and societal effects we may always be surprised by technology and its application in the field of politics, and social interaction.”*

Prof. Dr.-Ing. Christian Grimme, Head of the Computational Social Science & Systems Analytics (CSSSA) research group, WWU Münster



lyzed. This is probably due to the lack of sensational character of the really alarming developments.

It is much less a possible, presumed takeover of world domination by computers, malicious AI with consciousness, or the extinction of humanity by machines that is worrying, but rather seemingly banal developments. AIs with the ability to imitate voices are now able to reproduce the sound, intonation, speech flow, and even the finest phonetic specifications of real people. They can then even sing and repeat any desired lyrics without a human listener being able to tell that it is an imitation. This can be used for humorous purposes, such as having the late cult musician Johnny Cash sing the song “Barbie Girl”. However, this technology can also be used to post fake spoken comments, commit phone fraud, and in the worst case, bypass voice recognition in security devices.

Similarly, AI can be used to forge documents, develop malware, and even, through certain manipulations, assist in bomb making. However, these possibilities are not yet well explored and do not have a reliable empirical evidence base. It is simply too early to foresee exactly which potentially dangerous applications will actually be implemented. This is the risk of technological progress, that not everything is predictable and assessable and this is also the reason why AI is not (yet) discussed in detail in this compendium.

### Further Readings on that topic:

**Oxford Economics:** What automation really means for jobs and productivity. June 26, 2023.



**Pew Research Center:** Public Awareness of Artificial Intelligence in Everyday Activities. By Brian Kennedy, Alec Tyson and Emily Saks. February 15, 2023.



*engines, (symbolic) reasoning and expert systems;*  
**(c) Statistical approaches, Bayesian estimation, search and optimization methods.**

The EU AI act proposal seeks to address the potential negative impacts of AI on fundamental rights, including human dignity, privacy, and personal data protection. It also extends protection to special groups, such as workers, consumers, children, and individuals with disabilities.

A risk-based and proportionate approach is taken in this proposal to establish consistent AI regulations throughout the EU. Predictability and proportionality are ensured through a unified definition of AI, a robust risk assessment method, and clear obligations for AI system providers and users.

These rules will be enforced at both the Member State and Union levels, with a cooperation mechanism. These regulations will not apply to AI systems already on the market for at least one year before the new act takes effect. To achieve the general objective of the proposal, four policy options were examined by the Commission, including:

- voluntary labelling scheme
- sectoral “ad hoc” approach,
- horizontal EU legislative instrument with a proportionate risk-based approach
- mandatory requirements for all AI systems.

Following consideration of all four approaches, the decision was made to favor a horizontal EU legislative instrument that only includes high-risk AI systems and implementations. The purpose was to avoid unnecessarily slowing down AI development, research, and implementation.

In order to use or create AI applications with a high risk to citizen safety or fundamental rights, organizations must meet distinct responsibilities and duties.

As “high-risk” applications are defined (examples):

- Personal rights: AI systems using biometric data (e.g. public surveillance), systems for evaluation of the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such
- Infrastructure: AI as part of security systems surveilling road traffic and the supply of water, gas, heating and electricity
- Work: AI systems intended to be used for work recruitment, review of job applications, promotions, termination etc.

- Law enforcement: AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons, further systems intended to be used by law enforcement authorities for profiling of natural persons
- Justice: AI systems intended to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts.

The proposed act places limitations on the freedom to conduct business and the freedom of art and science to ensure compliance with public interest concerns, including health, safety, consumer protection, and fundamental rights. These limitations are proportionate and designed to impose the minimum necessary measures to prevent and mitigate serious safety risks. Each member state will be required to establish facilities and structures for assessing AI capabilities, and developers must fully cooperate with these newly established bodies.

The act prohibits certain AI applications in the EU, such as the use of subliminal techniques beyond an individual’s awareness and the exploitation of vulnerabilities in specific groups of people, like those based on age or physical or mental disability, which could cause physical or psychological harm. Public authorities are also barred from using AI systems to assess individuals based on their social behavior or known/predicted personal traits. Additionally, “real-time” remote biometric identification systems for law enforcement purposes in publicly accessible spaces are not allowed and must adhere to appropriate safeguards to protect citizens’ personal rights. Any AI system used for security purposes is classified as a high-risk system under this proposal.

## Directive on attacks against information systems

As part of the directive, various offenses directed against information systems will be criminalized and penalized, including botnets, which are defined by the EU Commission as: malicious software used to remotely control computer networks.

EU countries are also encouraged to use the same contact points as the Council of Europe and the G7 to address advanced technology threats. The directive covers a range of criminal offenses, from denial of ser-

vice attacks that aim to bring down a server to the interception of data and botnet attacks. To effectively combat cybercrime, all member states must criminalize the same offenses and provide law enforcement authorities with the tools to collaborate.

The member states have to harmonize their legislation and institutional capabilities for the enhancement of cooperation between judicial authorities concerning:

#### ■ **illegal access to information systems**

Member states must criminalize intentional unauthorized access to an information system, at least for significant cases involving the infringement of a security measure.

#### ■ **illegal system interference**

Member states must criminalize intentionally serious hindering or interrupting of an information system's functioning without right, at least for non-minor cases.

#### ■ **illegal data interference**

Deleting or damaging computer data intentionally and without right, rendering it inaccessible, or altering or suppressing it, shall be a punishable criminal offence in member states, at least for cases that are not minor.

#### ■ **illegal interception**

Member states must make it a criminal offence to intercept non-public transmissions of computer data to, from, or within an information system, including emissions from the system, intentionally and without right, at least for cases that are not minor.

A novelty is, that this directive as well introduces the liability of so called "legal persons" (companies, organizations, enterprises, etc.) to this law, and emphasizes, that instigating, aiding, abetting and attempting to commit cyber offenses will be as well prosecuted.

### **Tackling online disinformation: a European Approach**

In the eyes of the EU Commission it's not possible to find a single solution that can solve all the issues related to disinformation, but that it's not acceptable to do nothing about it on the other hand. This is the reason, why it provided a plan with four points, that lay out a plan for further action.

- Increase of transparency regarding the production, sponsorship, dissemination, and targeting of information in order to allow citizens to evaluate the content they access online and expose any potential attempts to manipulate opinion.
- Promoting information diversity, empowering citizens to make informed decisions through critical

thinking. This will be achieved by supporting high-quality journalism, media literacy, and rebalancing the relationship between information creators and distributors.

- Improvement of the credibility of information by indicating its trustworthiness through trusted flaggers and enhancing the traceability of information, as well as the authentication of influential information providers.
- Creation of inclusive solutions that involve raising awareness, increasing media literacy, involving various stakeholders such as public authorities, online platforms, advertisers, trusted flaggers, journalists, and media groups. These solutions aim to be effective and long-term.

Strongly connected to these provisions is the EU GDPR (General Data Protection Regulation) in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA), because it will include social media platforms and the identification of the accounts active on it. To address the problem of disinformation, it is necessary in the opinion of the EC to create a more transparent, trustworthy, and accountable online environment, as well as to improve our ability to fact-check information and develop collective knowledge about disinformation. This can be achieved by utilizing new technologies and tools.

Further it will set steps in motion, to require social media platforms to achieve the following goals:

- Improved scrutiny of advertisement placements, particularly to reduce revenues for purveyors of disinformation, and to significantly restrict targeting options for political advertising.
- Significantly improve transparency about sponsored content, especially in regards to political and issue-based advertising;
- Intensify and demonstrate the effectiveness of efforts to close fake accounts to increase transparency;
- Facilitate users' assessment of content through indicators of the trustworthiness of content sources, significantly improving their ability to identify reliable information; e.g. with fact checkers
- Dilute the visibility of disinformation through measures such as reducing their reach and prevalence on online platforms;
- Empower users to report disinformation, significantly increasing their role in identifying and combating false information;

- Ensure that online services include safeguards against disinformation, and provide trusted fact-checking organizations and academia with access to platform data, while respecting user privacy, trade secrets, and intellectual property.

The EC further aims to encourage the adoption of Internet Protocol version 6 (IPv6) and enhance the efficiency of the Domain Name and IP WHOIS systems, in order to detect, analyze and deter malicious online behavior on social media and beyond. Additional to that the EC will encourage eIDAS (electronic identification, authentication and trust services) to promote voluntary online systems for the identification of suppliers of information based on trustworthy electronic identification and authentication means.

## EU Digital Services Act (DSA)

The main goal of the DSA is to establish consistent regulations that promote a secure, reliable, and trustworthy online environment for social media services (called intermediary services), which will help to enhance innovation and safeguard fundamental rights, such as the principle of consumer protection.

It deals first with exemptions from liability of the providers of such platforms, in order to protect them from legal responsibility for content that they did not put on their social media service themselves. Further, it addresses the due diligence obligations by these companies (if they are active within the EU) concerning certain aspects, with a special section on the rules of implication of the provided regulation.

### Providers are not liable for:

- Mere conduit: messages and content that was not created and transmitted by him
- Caching: as long as the content is only temporarily stored for functional reasons, and not altered by him
- Hosting: as long as the content is not knowingly illegal and in case removes it from the platform

### Providers are responsible to:

- Remove content that is deemed illegal by the legislation of the member states and inform the relevant authorities
- Provide a reliable contact office that communicates with the authorities and the citizens
- Set clear terms of condition for the usage of their platform and make them transparent for everyone

**The regulation (GDPR)** came into effect in 2018, replacing the 1995 Data Protection Directive. It addresses data protection issues on the levels of ordinary citizens, organizations, as well as the member states themselves.

The regulation aims to give citizens more control over their personal data, by introducing stricter rules on the collection, use, and storage of personal data by organizations. Under the GDPR, personal data includes any information relating to an identified or identifiable natural person, such as name, address, email address, identification number, location data, and online identifiers.

GDPR applies to all organizations that collect or process personal data of EU residents, regardless of where the organization is based. It also applies to organizations outside the EU if they offer goods or services to EU residents or monitor the behavior of EU residents. The regulation establishes a set of data protection principles and rights for individuals, including the right to access, rectify, and erase personal data.

Each EU member state has an independent supervisory authority responsible for enforcing the GDPR. Organizations that fail to comply with the GDPR can face significant fines, up to 4% of their global annual revenue or €20 million, whichever is higher.

The GDPR also includes provisions on data breach notification, data protection impact assessments, and the appointment of data protection officers for certain types of organizations. It aims to promote transparency and accountability in the handling of personal data and to consolidate trust between individuals and organizations.

- Implement sanctions against illegal activities (content removing, suspension, blocking, demonetization, legal actions, etc.)
- Actively seek the help of users to flag illegal content and provide reasons to trespassers why their content was removed
- Special trusted flaggers should be encouraged and engaged to act as independent auxiliaries based on their expertise in a certain social field to identify harmful and illegal content



It is worth noting, that so called handlers of designated “very large online platforms” (by definition having equal to or more than 45 million constant users, e.g. Twitter, Google) have to deliberately disclose any possible source of danger for the EU and its member states (especially when it comes to possible manipulations of elections). Especially inauthentic and malicious automated behavior has to be reported and addressed, for example by removing the accounts that show these features. Further those companies will have to work proactively with EU institutions (Digital Service Coordinators, or the European Commission) on the mitigation of such risks, to develop a crisis response mechanism, and upon request to open their data set for scrutiny and monitoring. The expenses for these steps are to be covered by the providers themselves.

In case that these service companies do not comply with these provisions, severe penalties are entrenched in the DSA, for example periodic payment that shall be 5 % of the average daily worldwide turnover or income of the provider of intermediary services concerned in the preceding financial year per day.

## Sources and Further Readings:

### Digital Services Act



### Artificial Intelligence Act:



### Cyber Resilience Act:



### Directive on attacks against information systems



### NIS2



### GDPR



## 2. NATO

NATO has made cyber defense a core part of its collective defense responsibilities, with a focus on educating personnel, providing training, and conducting exercises. The organization operates 24/7 to assist allies in preventing, mitigating, and recovering from cyber attacks. In 2018, member nations established a Cyber-space Operations Centre and approved a NATO guide to enhance its response to cyber threats.

In 2014, NATO implemented a policy and action plan to bolster its cyber defense, emphasizing the relevance of international law in cyberspace and promoting collaboration with the private sector.

At the 2021 NATO Summit, a Comprehensive Cyber Defense Policy was approved to actively prevent, defend against, and counter a wide range of cyber threats across political, military, and technical levels.

The Cyberspace Operations Centre, established in 2018, enhances situational awareness and coordinates NATO's cyber efforts. Allies agreed that NATO could use national cyber capabilities for operations while retaining ownership of these contributions.

NATO has expressed concerns about Russia's increased hybrid activities, including interference in democratic processes, political pressure, disinformation campaigns, malicious cyber activities, and cyber criminal operations. NATO stands in solidarity with impacted Allies.

Effective command and control are crucial for NATO's ability to handle simultaneous challenges. The NATO Cooperative Cyber Defence Centre of Excellence and other entities have achieved Initial Operational Capability. Allied contributions to command and control, along with host nation support, enhance the alliance's readiness and capability to respond to threats from any direction.

### NATO Stratcom

NATO Strategic Communications Centre of Excellence is a multinational and NATO-accredited international military organization, not part of the NATO Command Structure nor subordinate to any other NATO entity. NATO does not speak through the Centre.

Riga, Latvia, hosts NATO's StratCom COE, which improves the Alliance's and Allied nations' strategic communications capabilities. The Alliance's political

In order to understand the various NATO exercises, it is necessary to comprehend the settings. Those are organized in certain settings: Blue team vs. red team: The first one acts as the defender, the latter as the adversary Red team setting: One team acting as adversary probes the structures of the alliance in order to improve security measures

and military objectives are accomplished through strategic communication, so it is increasingly important that it communicates about its evolving roles, objectives and missions in a timely, accurate, and responsive manner.

As part of its mission, the Centre aims to contribute substantially to NATO's strategic communications capabilities, as well as those of its allies and partners. Its strength lies in its multinational and cross-sector participation from the civilian, military, private, and academic sectors, and the use of cutting-edge technologies. The NATO StratCom COE is made up of a diverse group of international experts – trainers, educators, analysts, and researchers from military, government, and academia.

Participants and sponsoring nations provide the Centre with staff and funding. It was founded in 2014 by Latvia, Estonia, Germany, Italy, Lithuania, Poland, and the United Kingdom. Finland and the Netherlands joined in 2016, Sweden in 2017, Canada in 2018 and Slovakia in early 2019. The USA and Denmark joined in 2020. It is expected that Hungary will join the EU in 2021, but France and Australia have already begun the application process.

### Major Products and Activities in 2021

- NATO StratCom policy & doctrine development
- Multinational Information Operations Experiment (MNIOE)
- Multinational Capability Development Campaign (MCDC)
- Analysing counter-narrative strategies, narrative development and assessment
- StratCom tabletop exercise (TTX) concept development and information environment simulation concept development
- Concept development of the disinformation attack simulation training module
- NATO Warfighting capstone concept development

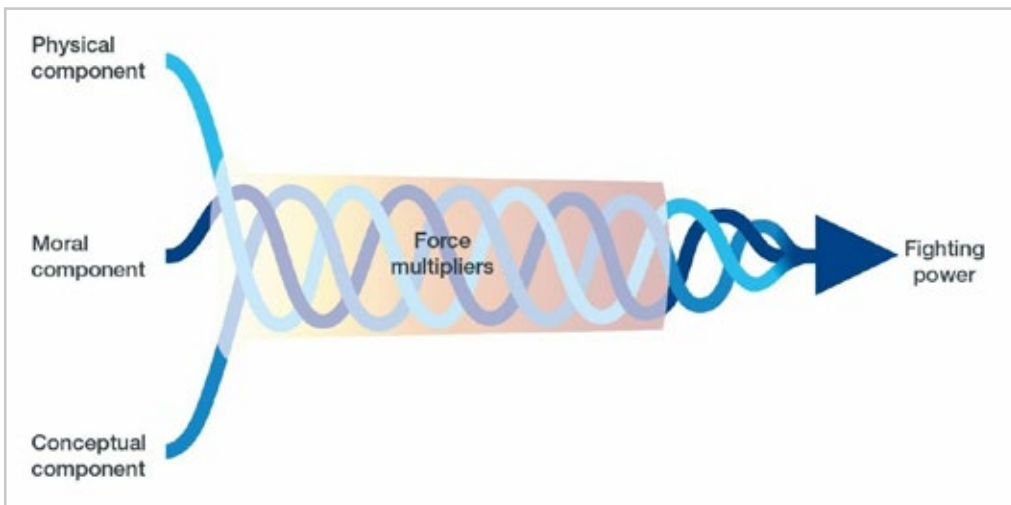


Figure 15: General NATO Fighting Power doctrine as well relates to the Cyberspace: Moral (cognitive aspect) physical component (military IoT devices) and conceptual component (Joint all Command and Control)

- Work on StratCom Terminology Improvement
- Social media course and conference
- StratCom education and training support to ACT

### NATO Cyber Security Centre

The NATO Cyber Security Centre, formerly known as the NATO Computer Incident Response Capability Technical Centre (NCIRC TC), is in charge for the full lifecycle of NATO’s cyber security activities, designing, implementing and operating:

- Scientific and technical expertise
- Supporting Acquisition, Maintenance and Sustainment
- Conducting Operations and Incident Response / CERT

One main part of this is the Communication and Information Agency (NCI)

The NCI Agency Cyber Security Service Line is responsible for NATO’s first line of cyber defense, working to develop cyber defense capabilities and operating the NATO Information Security Operations Centre and the NATO Computer Incident Response Capability (NCIRC) Technical Centre. The Cyber Security Service Line provides integrated cyber defense around the clock, year-round, and is responsible for all lifecycle management activities, including research and development, subject matter expertise, software development, acquisition, and operations and maintenance.

The establishment of the Agency is part of a broader NATO reform:

- The new NCI Agency “connects forces, NATO and Nations”- it is NATO’s IT and C4ISR provider, including cyber and missile defense.

- It is a key pillar of NATO Secretary General’s Smart Defense and Connected Forces initiatives; Supporting NATO operations is its top priority.

The Cybersecurity Service Line Operations Branch provides a range of measures aimed at preventing, detecting, responding to, and recovering from cyber attacks and incidents. These services are focused on cryptography, identity management, round-the-clock operational support for cyber security, incident handling, technical services to support cyber security operations, and cyber security support for deployed operations and exercises.

*“We finally need to comprehend, that democracy is a critical infrastructure of by itself.”*

Dr. Ross King, Head of Competence Unit, Data Science & Artificial Intelligence, Austrian Institute of Technology (AIT)

### ■ The NATO CCDCOE

In 2003, Jaap de Hoop Scheffer, the Secretary-General of NATO, lent his support to Estonia’s suggestion for a Centre of Excellence. Subsequently, during the 2008 NATO summit in Bucharest, NATO expressed its willingness to provide assistance to its allied nations in countering cyber attacks, subject to their request.

The Cyber Defense Center located in Tallinn is among the 21 Centers of Excellence (COEs) that have received accreditation for training in the technically advanced

## Cognitive Warfare in the Digital Era

With the proliferation of information and the interconnectedness of the digital world, cognitive warfare has become a powerful tool for state and non-state actors to advance their strategic objectives. Maintaining national security and stability in an increasingly complex global landscape requires understanding and countering this form of warfare.

For instance, in the United States, the Depart-

example, in the 2008 war between Russia and Georgia, Moscow used a combination of cyber-attacks, state-controlled media, and disinformation to project a narrative of a Russian peacekeeping mission while simultaneously destabilizing its adversary<sup>29</sup>.

### Key Elements:

- Psychological Operations (PSYOP): Psychological tactics, such as persuasive messaging, fear, and emotional manipulation, are used to influence people's decisions.

- Information Warfare: The spread of information, misinformation, disinformation, and propaganda through various channels, including social media, news outlets, and online platforms. Public opinion is manipulated and dissent is sow. Targets are societal divisions, friction lines along political opinions in order to increase tribalism and polarization.

Cyber Operations: An adversary's information systems can be disrupted, chaos created, and trust undermined through cyberattacks, hacking, or data breaches.

Social Engineering: By utilizing social engineering tech-

*“For NATO and its allied Nations it’s yet unclear to what degree they are legitimized to engage in this form of cognitive warfare. Most techniques mentioned before run contrary to democratic norms and values, leaving this battlefield more open for autocratic regimes. While there are still many legal and ethical questions to solve, it is clear that NATO does not have the option to avoid cognitive warfare altogether. If an adversary chooses the cognitive domain for warfare, NATO has no choice but to react at least in a matter of defense and cognitive security.”*

LTC Dr. Soenke Niedringhaus, Bundeswehr, NATO StratCom

ment of Defense has made countering cognitive warfare a priority, creating a new office dedicated to the task.

In order to achieve strategic objectives, it manipulates and exploits the cognitive processes of an adversary, such as perception, decision-making, and beliefs. A cognitive war operates primarily in the cognitive domain, aiming to influence and control individuals and groups' minds, rather than traditional warfare, which relies on physical force and weapons. For

niques, attackers can manipulate individuals into divulging sensitive information or performing actions beneficial to their objectives through cognitive warfare.

### Objectives:

- Influence and control over specific groups within the advisory population
- Deception of the enemy
- Disruption of decision-making processes

## STATE OF PLAY

aspects of NATO operations. The Center is currently funded by multiple nations, including national and multi-national funding.

In addition to its role in providing training, the Cyber Defence Center in Tallinn has various other responsibilities as well. These include the development of cyber defense practices and standards, contributing to the formulation of NATO security policies, conducting training sessions, awareness campaigns, workshops and courses, and providing support for cyber defense exercises.

### DIANA

NATO has established a transatlantic innovation ecosystem to leverage the latest technology for security and defense purposes, as agreed at the 2021 Brussels Summit. As part of this initiative, NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) has grown to include over 100 affiliated accelerators and test centers across almost all Allied countries, including CR14 in Tallinn, which is used for cyber-defense testing.

Recently, DIANA's Board of Directors has expanded the network by adding 28 deep-tech test centers across several Allied countries and two new startup accelerator sites in North America. This expansion is a significant step towards harnessing the latest technology for NATO's security and defense, building a unique transatlantic innovation ecosystem.

Starting in autumn 2023, DIANA will implement its first challenge programs in cooperation with the following accelerator sites, pending conclusion of the necessary contractual arrangements:

- Tehnopol in Tallinn;
- Officine Grandi Riparazioni (OGR) in Turin;
- BioInnovation Institute (BII) in Copenhagen;
- MassChallenge in Boston;
- Pacific Northwest Mission Acceleration Center (PNMAC) in Seattle.

Current exercises of various NATO bodies

### Cyber Coalition

NATO recently completed its largest annual cyber defense exercise called Cyber Coalition 2022, which is as well labelled as the flagship exercise of the alliance. Over 1,000 cyber defenders from 32 countries participated in the scenario, which tested their ability to prevent attacks and intrusions. The exercise was led by

NATO's Allied Command Transformation based in the USA and experimented with using artificial intelligence to counter cyber threats, standardizing information-sharing during a cyber crisis, and exploiting intelligence to improve shared situational awareness. Cyber Coalition 22 involved 26 NATO Allies and several partners, including Finland, Sweden, Georgia, Ireland, Japan, Switzerland, and participants from the European Union, industry, and academia. The exercise is considered one of the largest cyber defense exercises in the world.

The exercise took place from 29 November to 3 December 2021 and aimed to enhance collaboration within

- NATO's cyberspace domain
- improve operational capabilities
- Provide input for the NATO Cyberspace Transformation.

Participants included NATO bodies, allied nations, and partner countries, with the goal of strengthening the alliance's ability to defend against cyber threats in support of its core tasks. The exercise tested decision-making processes, technical and operational procedures, and the capabilities of NATO and national cyber defense systems.

### Locked Shields

Since 2010, the CCDCOE has been organizing the Locked Shields exercise, which provides an opportunity for cyber security experts to improve their skills in defending national IT systems and critical infrastructure against real-time cyber attacks. It is as well the world's largest exercise of such kind.

The last issue of the exercise involved 22 Blue Teams and 5000 virtualized systems that are subjected to more than 4000 simulated cyber attacks.

It further included the cooperation with civilian enterprises and governmental organizations like Siemens, TalTech (Tallinn University of Technology), Clarified Security (Cybersecurity company, Estonia), Arctic Security (Cybersecurity company, Finland), and CR14 (Foundation of the Estonian Ministry of Defense).

Locked Shields is a classical red team (adversary) vs. blue team (defender) exercise, including 50 experts on both sides, competing over two different objectives, that is to assist a fictive country to fend off a massive cyberattack on its critical infrastructure (energy, water supply, heating, traffic, etc.), or to find weak points

within the defending team. The exercise had 5500 virtual systems and 8000 attacks. The participating teams had to:

- secure complex IT systems
- handle incident reporting
- handle forensic and legal challenges
- deal with media and information warfare issues.

Every year, the Locked Shields exercise brings together participants from 32 nations to practice defending national IT systems and critical infrastructure against large-scale cyber attacks in a live-fire scenario. The exercise involves around 2,000 participants and tests their skills and readiness to protect against simulated cyber threats.

The simulated scenario in 2022 was the following:

***Fictional island country Berylia faces coordinated cyber-attacks causing disruptions to government and military networks, communications, water and power systems, leading to public unrest. Exercise includes simulating a central bank's reserve management and financial messaging systems, and deploying a 5G Standalone mobile communication platform as part of critical infrastructure.***

### **Crossed Swords**

Crossed Swords is an annual cyber exercise that provides technical training for penetration testers, digital forensics experts, and situational awareness experts. It has expanded over the years to include:

- leadership training
- legal aspects
- joint cyber-kinetic operations

The exercise also serves as a training opportunity for Red Team members who play the adversary in the Locked Shields cyber defense exercise.

In 2021 the exercise took again place at the CR14 training site in Tallinn after a two years hiatus because of the Coronavirus Pandemic and it included one hundred participants from 21 countries, both NATO and non-NATO countries.

Crossed Swords is a so-called “red teaming cyber exercise” that has expanded significantly in scope and complexity since 2018, covering multiple geographical areas and including critical information infrastructure providers and military units. As of 2019, a dedicated cyber command element is included in the exercise’s training audience. With over 100 experts from 23 coun-

tries participating, Crossed Swords 2019 was the largest and most complex exercise in the series to date.

### **Cooperation through intergovernmental bodies: PESCO – Linking between NATO and the EU**

The European Union’s Permanent Structured Cooperation (PESCO) is a framework that aims to enhance defense cooperation between participating EU Member States

Projects within the framework are assessed thoroughly from both the capability and operational perspective, with the objective of supporting capability development and providing substantial support to Common Security and Defense Policy operations and missions. PESCO is complementary to other initiatives such as the European Defense Fund and the Coordinated Annual Review on Defense (CARD), which support collaborative initiatives and the identification of opportunities for new projects.

There are several touching points and linkages that seek to improve the cooperation and joint activities of NATO and the EU, this covers as well significant projects and initiatives on the cyber level:

### **CYBER RAPID RESPONSE TEAMS AND MUTUAL ASSISTANCE IN CYBER SECURITY (CRRT)**

**Coordinator:** Latvia

**Members:** Belgium, Estonia, Croatia, Latvia, Netherlands, Poland, Romania, Slovenia

The establishment of Cyber Rapid Response Teams (CRRTs) marks a significant step towards achieving a higher level of cyber resilience among member states of the EU. These teams will enable countries to provide mutual assistance and collaborate in responding to cyber incidents. The CRRTs can be used to support member states, EU Institutions, CSDP operations (Common Security and Defense Program), as well as partners, and will be equipped with a commonly developed deployable cyber toolkit that is designed to detect, recognize, and mitigate cyber threats.

These teams will be able to offer training, vulnerability assessments, and other forms of support as requested. The experts from participating member states will work together to pool their resources and provide a coordinated response to cyber incidents. The ultimate goal of the CRRTs is to enhance the collective cyber defense capabilities of member states and ensure that Europe is better prepared to tackle cyber threats.

## STATE OF PLAY

It is foremost CSDP where NATO and EU member states cooperate within this project.

### **CYBER AND INFORMATION DOMAIN COORDINATION CENTER (CIDCC)**

#### **Coordinator:**

The aim of the project is to create and manage a permanent multinational military unit called the Cyber and Information Domain Coordination Center (CIDCC), which will coordinate and respond to cyber threats and incidents. The participating member states will contribute national staff to the center and will have the sovereign decision-making power to decide which threats, incidents, and operations they will provide resources and information for. This approach aligns with the European resolution of 13 June 2018 on cyber defense.

### **CYBER THREATS AND INCIDENT RESPONSE INFORMATION SHARING PLATFORM (CTIRISP)**

The Cyber Threats and Incident Response Information Sharing Platform aims to enhance the cyber defense capabilities of member states by facilitating the sharing of cyber threat intelligence through a networked platform. This project is intended to mitigate risks associated with cyber threats and incidents by enabling the development of more active defense measures, which may go beyond the use of firewalls.

### **CYBER RANGES FEDERATIONS (CRF)**

The main goal of the project is to strengthen the European Cyber Ranges by integrating individual national Cyber Ranges into a larger cluster with greater capacity and specialized services. This will allow the sharing and pooling of capabilities, resulting in improved quality of cyber training and exercises. Furthermore, the federation can be utilized for research and development activities related to cybersecurity.

## Sources and Further Readings:

### **NATO Stratcom**



### **NATO Cyber Defense:**



### **NATO NCI:**



### **NATO CCDCOE:**



### **NATO DIANA**



### **NATO Locked Shields**



### **NATO Crossed Swords**



### 3. Germany – Back to base: a country in the crosshairs buckling up for the worst

How is Germany defending itself? How is it positioned and what new initiatives are there?

Ensuring national security and protecting citizens from threats in the digital space is a key responsibility of the German government. The Federal Ministry of the Interior and Homeland is tasked with overseeing cybersecurity measures within the federal government.

Two years ago the German government adopted a new “Cybersecurity Strategy for Germany 2021”. These are the main principles:

#### 1. Establishing cybersecurity as a joint task of the state, economy, science and society

In a nutshell, this point addresses the linkage of national German cybersecurity with partners within the economy, civil society organizations, civic organizations, academia, as well as connecting it with “the bigger context” within EU and NATO.

#### 2. Strengthen the digital sovereignty of government, business, science and society

Digital sovereignty is therefore a central guideline of the Cybersecurity Strategy 2021 and a motif for action in all four fields of action.

- Field of action 1: application-oriented research and development as well as research transfer
- Field of action 2: cybersecurity as a quality feature “Made in Germany”
- Field of action 3: government capabilities for assessing new technologies and commissioning European providers and for self-assurance of the administration
- Field of action 4: a common EU vision and strategy for cybersecurity and European digital sovereignty

The German government is focused on protecting security interests, digital sovereignty, and resilience against hybrid threats, as well as reducing reliance on foreign information technologies. In addition to existing review mechanisms, such as those under the Foreign Trade and Payments Act and the Foreign Trade and Payments Ordinance, the government is developing flexible and strategically deployable instruments to respond to potential divestments of key security and defense industrial technologies. One such instrument is the establishment of an IT security fund, which aims to actively counteract unwanted takeovers.

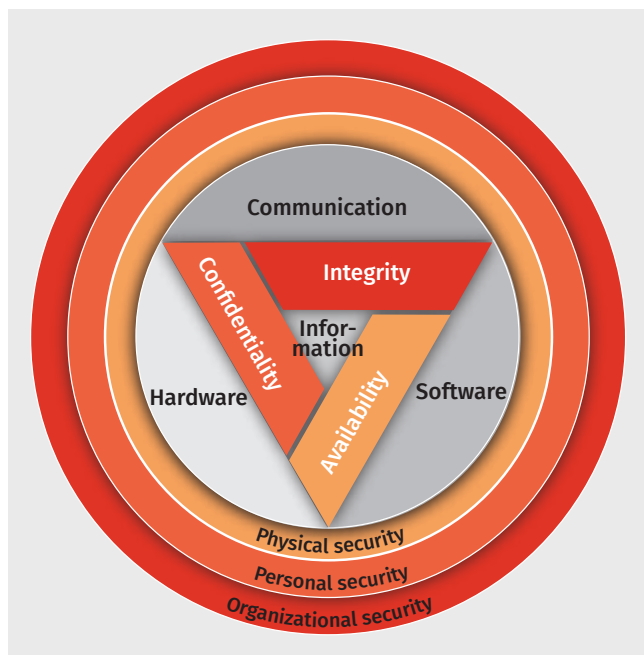


Figure 16: Security triangle in the area of digital-information. Courtesy of the Central Intelligence Agency (CIA)

The German government has initiated the “StartUp-Secure” program to accelerate the implementation of marketable ideas in the field of IT security. The program focuses on supporting start-ups in the IT security industry, and the national competence centers for IT security research – ATHENE (Darmstadt), CISPA (Saarbrücken), KASTEL (Karlsruhe), and the Ruhr University Bochum – are involved in supporting young start-ups.

The IT Planning Council adopted the “Strategy to Strengthen Digital Sovereignty for IT in Public Administration” in March 2021, with the aim of strengthening the digital sovereignty of public administration. The strategy includes strategic goals such as “changeability,” “design capability,” and “influence on providers,” and outlines various approaches and measures for achieving these goals. One of the measures is diversification through the use of open source IT solutions that are tailored to the needs of public administration. In addition, the “QuNET” initiative, which is funded by the German government and involves the Fraunhofer-Gesellschaft, the Max Planck Society, and the German Aerospace Center, has been developing technologies for a pilot network for quantum communication in Germany since the end of 2019. This network is intended for secure data transmission in the future.



### 3. Shaping safe digitalization

The German government has taken steps to drive the digital transformation in the country through different initiatives and measures. One of these is the “Digitalization Shaping Digitization” strategy, which outlines key projects to implement digital policies in areas such as digital skills, infrastructure, digital transformation of the state and society, and ethics for a digital society.

- The University of the Bundeswehr Munich has a cyber cluster for research and development, scientific training, and further education in cybersecurity, particularly for officers and federal employees.
- The German government has introduced a research framework program called “Digital. Secure. Sovereign.” that focuses on IT security.
- The cyber agency has been established to conduct interdepartmental research projects with significant innovation potential in cybersecurity and related key technologies to address the security needs of Germany internally and externally.

The German government has revised and updated its network strategy with the “Network Strategy 2030 for Public Administration”. This new strategy aims to establish an information network of the German public administration (“IVÖV”, Informationsverbund öffentliche Verwaltung) under the operational responsibility of the federal network operator (BDBOS), taking into account the increased requirements for communication capability, new technical developments and the increased security requirements. The strategy defines five strategic goals, including national digital sovereignty, network infrastructure performance, information security and data protection, future viability and flexibility, and digital collaboration.

To achieve these goals, the strategy identifies seven strategic action areas, including vertical integration, active service provider management, network consolidation, internet resources and standardization, information security and data protection, user and service management, and promoting innovations for a citizen-centric and modern administration. By implementing these action areas, the “Network Strategy 2030 for Public Administration” aims to contribute to ensuring cybersecurity in Germany.

### 4. Make goals measurable and transparent

The Cybersecurity Strategy 2021 consists of both strategic goals and operational measures. The strategic goals are specific, measurable, actively influenceable, realistic, and timed objectives that aim to address the

challenges of the field of action and describe a targeted state. Each strategic goal has defined indicators for measuring its achievement, and they are generally expected to be achieved within a five-year period. On the other hand, measures describe activities that are planned to achieve the strategic goals. These measures should be suitable for fully achieving the respective strategic objectives within the timeframe of the Cybersecurity Strategy 2021. Measures can be either individual projects or ongoing activities that are planned and implemented downstream as part of the strategy.

#### Federal Office for Information Security (BSI)

The BSI, which is the federal government’s cybersecurity agency, plays a vital role in shaping information security in the digital age by providing prevention, information, detection and response measures. It has established itself as a nationally recognized competence center, and its expertise benefits the state, businesses and society directly. The range of services offered by BSI includes defending against cyber attacks, providing consultancy services, developing security-related recommendations, best practices and standards, and certification.

BSI also supports the entire federal administration by maintaining the Computer Emergency Response Team Bund (CERT Bund) and Mobile Incident Response Teams (MIRT). In addition, it operates the National IT Situation Center, which is in constant communication with the Joint Federal and State Reporting and Situation Center.

#### Federal Criminal Police Office (BKA)

The Federal Criminal Police Office (BKA) plays a crucial role as the primary law enforcement agency responsible for investigating a broad range of cybercrimes, a type of criminal activity that is expanding at an unprecedented rate. By assuming this responsibility, the BKA provides national coordination, conducts centralized investigations of cybercrime phenomena, performs operational assessments, and establishes strategic partnerships.

#### Federal Office for the Protection of the Constitution (BfV)

The swift and continuous evolution of information and communication technologies has enabled foreign intelligence services and other malicious actors to engage in espionage, disinformation campaigns, data tampering, and computer sabotage. These activities target government and social institutions, research

facilities, and businesses, with both large corporations and small to medium-sized enterprises being equally vulnerable. Given its role in the European Union and NATO, its geopolitical position, and the presence of many high-tech companies, Germany is a frequent and appealing target for such attacks. The Federal Office for the Protection of the Constitution (BfV) responds to this threat environment by promptly and effectively identifying and countering cyber attacks and their potential sources.

### **National Cyber Defense Center (Cyber-AZ)**

The National Cyber Defense Center, also known as Cyber-AZ, aims to improve operational cooperation and coordinate protection and defense measures among multiple security agencies to counter cyber attacks. The sharing of knowledge among authorities in their respective areas of responsibility is expected to bring benefits. At present, Cyber-AZ includes the following represented authorities:

- Federal Office for Information Security (BSI),
- Federal Criminal Police Office (BKA),
- Federal Police (BPol),
- Federal Office for the Protection of the Constitution (BfV),
- Federal Intelligence Service (BND),
- Federal Office for Military Counterintelligence (BAMAD),
- Federal Office of Civil Protection and Disaster Assistance (BBK),
- Customs Criminal Investigation Office (ZKA),
- Federal Armed Forces (BW)
- Federal Financial Supervisory Authority (BaFin)

### **Central Office for Information Technology in the Security Sector (ZITiS)**

The Central Office for Information Technology in the Security Sector (ZITiS) is a central service provider that offers support and advice to federal authorities on information technology related security tasks. ZITiS achieves this by pooling expertise, conducting centralized research on new technologies, and developing methods and tools that aid federal authorities in investigations and reconnaissance related security tasks.

### **Agency for Innovation in Cyber Security (Cyber Agentur)**

The Cyber Agency is a newly established limited liability company of the Federal Government with the objective of achieving greater technological sovereignty in cybersecurity and mitigating the risk of dependence on foreign know-how. The agency does not conduct

research on its own, but collaborates with experts from government agencies and institutions to identify crucial technologies and innovative potential in cybersecurity. The Cyber Agency then develops programs and projects that are put out for tender to external partners.

### **Current projects by the German government and its federal institutions**

#### **The National Cyber Security Council (NCSR)**

NCSR is a strategic advisory body that is chaired by the Federal Government Commissioner for Information Technology (BfIT) and facilitates cooperation in the field of cyber security between the federal government and the private sector. The NCSR identifies long-term trends and requirements, and provides recommendations to the Federal Government for strengthening cyber security based on these insights.

#### **Alliance for Cyber Security (ACS)**

The Alliance for Cyber Security (ACS) was established in 2012 by the BSI and the industry association BITKOM to bolster Germany's resilience as a business location against cyber attacks. The initiative currently boasts 3,876 participating companies, including manufacturers and service providers from the IT industry and user companies of all sizes and sectors, along with 110 other partners and 90 multipliers. The ACS provides a variety of exchange formats for participants, as well as institutionalized cooperation, a broad range of training courses, and up-to-date information and warnings from the BSI and industry partners.

#### **UP KRITIS**

UP KRITIS is a joint cooperation and information platform on IT security between critical infrastructure (KRITIS) operators and their regulatory authorities, encompassing public and private sectors. The initiative involves the Federal Ministry of the Interior and Homeland, the Federal Office for Information Security, and the Federal Office of Civil Protection and Disaster Assistance. The main aim of UP KRITIS is to ensure the continuity of critical infrastructure services across Germany. Participation is open to smaller KRITIS operators who are not subject to legal obligations. The BSI provides all UP KRITIS participants with IT security information and alerts.

#### **German Competence Centre against Cyber Crime (G4C)**

The German Competence Centre against Cyber Crime (G4C) is an autonomous operational association with several companies, mainly from the financial sector, as

its members. BKA and BSI collaborate with the G4C as partners. By sharing information on cybercrime trends and patterns, the G4C devises tools, methods, and suggestions for preventing cybercrime.

### **Task Force against Disinformation**

The task force UAG RUS/UKR was created by the Federal Ministry of the Interior and Homeland Affairs (BMI) as part of the interdepartmental Hybrid Threats Working Group (AG Hybrid) to ensure close interdepartmental and interagency exchange on identifying and countering hybrid threats, specifically disinformation, in relation to Russia's war in Ukraine. The task force focuses on identifying Russian narratives, promoting fact-based communication, and enhancing societal resilience against information space threats. The Federal Foreign Office (AA), the Federal Press Office (BPA), and the Federal Ministry of the Interior (BMI) and their subordinate agencies closely monitor the information space for false or misleading information and exchange information on this subject with other departments and agencies of the federal and state governments. The primary focus is on proactive and fact-based communication tailored to specific target groups regarding the current situation and the measures taken.

### **Further Readings:**

**Federal Minister of the Interior and Community: Cyber Security Strategy for Germany. September 08, 2021. In English.**



**Federal Office for Information Security (BSI) in English.**



**Federal Criminal Police Office (BKA) – Division CC: Cybercrime. In English.**



**Federal Office for the Protection of the Constitution (BfV) – Cyberdefense. In English.**



**Zitis – Central Office for Information Technology in the Security Sector. In English.**



**Agency for Innovation in Cyber Security (Cyber Agentur). In German.**



**The National Cyber Security Council (NCSR). In German.****Alliance for Cyber Security (ACS). In German.****UP KRITIS. In English.****German Competence Centre against Cyber Crime (G4C). In German.****Task Force against Disinformation. In English.****Global initiatives****UN Global Governmental Experts (UN GGE)/Open-Ended Working Group (OEWG) on information and telecommunication security**

The group initiated its efforts on June 1, 2021, and held an initial session for organization. The first substantial session was intended to occur in December 2021.

All UN member states are eligible to participate in the second OEWG and the group has engaged in consultative meetings with interested parties. Approval for participation in the group was granted on a ‘no objection’ basis. A permanent UN forum has been proposed by 40 states as a Program of Action to advance responsible state behavior in cyberspace.

States are called to engage in discussions regarding both existing and potential threats in cyberspace, and to implement their commitments based on the framework for responsible State behavior. Furthermore, states should also engage with relevant stakeholders in the process.

The UN General Assembly (UNGA) adopted all reports by consensus from all member states. In addition, various UNGA resolutions, such as those that created the GGEs and OEWGs on cybersecurity, also play a role. As in 2023 there have been four reports since 2013 on the sessions.

Despite three substantial sessions, the OEWG’s primary challenge remains the inclusion of non-state stakeholders in the OEWG process. Nonetheless, the group has made some advancements in confidence-building measures and capacity building.

**Results of the UN OEWG Report 2021**

The final report of the Open-ended Working Group (OEWG) on Developments in the Field of ICTs in the Context of International Security was adopted during its third and final substantive session. The report reiterated the conclusions of the previous reports of the Group of Governmental Experts (GGE) and emphasized that international law, including the Charter of the UN, applies to cyberspace. The report also stated that norms are not meant to replace or modify the binding rights and obligations of states under international law but rather provide specific guidance on responsible state behavior when using ICTs.

The report recommended that states should voluntarily identify and consider confidence-building measures (CBMs) that are relevant to their particular situations and cooperate with other states in implementing

them. It also provided comprehensive measures for capacity building in the field of ICT security. The report was adopted by consensus of all states.

### **GFCE – Global Forum on Cyber Expertise**

The Global Forum on Cyber Expertise (GFCE) is an international platform that focuses on strengthening global cooperation on cyber capacity building. The GFCE achieves this by coordinating various regional and global projects and initiatives, facilitating the sharing of knowledge and expertise among its members, and matching the specific needs for cyber capacities to offers of support from the community. Through these efforts, the GFCE aims to foster a safe and secure cyberspace globally.

The GFCE convenes meetings twice a year to evaluate advancements and engage in policy dialogues about how to address emerging issues in the area of cyber capacity building. These gatherings provide a platform for sharing ideas and best practices among participants.

The GFCE was founded in 2015 during the Global Conference on Cyber Space in The Hague, with the aim of enhancing cyber capacity building and improving coordination among existing international initiatives. In its initial phase, the GFCE focused on creating a strong network and raising awareness of ongoing global capacity building projects. In 2017, at the Global Conference on Cyber Space in New Delhi, the organization positioned itself as the coordinating platform for cyber capacity building by establishing the Global Agenda for Cyber Capacity Building, which prioritizes 11 topics under 5 themes. Working Groups were created to implement the Agenda, and the GFCE community contributed to their rapid development. In 2019, the institution shifted its focus to strengthening its ecosystem by developing a clearing house function, launching the Cybil Knowledge Portal, and becoming an independent, not-for-profit GFCE Foundation with a new governance structure. This enables the GFCE to become even more internationalized, accept funding from multiple donors, and work towards an effective clearing house mechanism and a Global Cyber Capacity Building Research Agenda.

### **Working groups of the GFCE:**

- A.** Cyber Security Policy and Strategy;
- B.** Cyber Incident Management and Critical Information Infrastructure Protection;
- C.** Cybercrime;
- D.** Cyber Security Culture & Skills;
- E.** Cyber Security Internet Standards

The GFCE comprises more than 180 Members and Partners from diverse stakeholder groups, including government, international organizations, industry, non-governmental organizations, academia, technical groups, and civil society. To enhance the network’s functionality, GFCE structures and groups are developed voluntarily by its members, which together make up the GFCE ecosystem that caters to the Community’s needs. These structures include Co-Chairs, Advisory Board, Working Groups Chairs, Research Committee, Cybil Steering Committee, Regional Hubs, and Liaisons. The GFCE Secretariat supports all of these structures.

### **Further Readings:**

**UN Open-Ended Working Group (OEWG) Report. March 12, 2021.**



**GFCE – Global Forum on Cyber Expertise**





Welcome to the jungle! At first glance, the multitude of ordinances, regulations and laws and countless organizations, institutions and working groups create a rather complex and sometimes confusing picture. In the next chapter, we will analyze this web in more detail.

# 10 Way ahead: Examination of the cyber strategies and policy suggestions for EU, NATO, Germany and the global level

---

So much is the state of the current institutional defenses, their reform and new projects that have been built, are being built and are being deployed in the fight against cyberattacks and disinformation. However, what about vulnerabilities that still exist and where criticism is needed? Cyberspace, in conjunction with social networks and artificial intelligence, which is now widely used, is the revolutionary socio-technological aspect for our future coexistence.

The concepts of securitization and actor-network theory have already been covered in this report, but we want to revisit them here in order to evaluate recent developments.

Two dynamics in particular should be taken into account when evaluating these processes. We want to call them negative and positive dynamics here, in order to be able to represent the possible developments better.

Abstracting dynamics in the current securitization and the actor network within the phenomenon we are considering are of a limiting character, that is, they restrict freedoms, regulate and prohibit activities and technologies. However, this designation is not a judgmental consideration but only represents the process of a deduction.

Progressive dynamics in the current securitization and actor network within the phenomenon we are considering are multiplicative in nature, meaning they build and perpetuate structures of societal and state resilience against attack.

Although at first glance cybersecurity and online disinformation may be perceived as separate phenomena, a close connection between the two emerged in our report.

## A. EU – Welcome to the Jungle

The European Union's current strategy is characterized primarily by creating "new structural capabilities," which in turn have a broadly abstracting effect. Most of the newly created institutions are aimed at limiting the choice of technologies available on the European market, or at regulating their use. The essential question here, however, is: Is this even possible in this form in a globally networked world?

According to the new cyber strategy of the European Union, manufacturers of software products are supposed to submit data on their self-developed products to the national bodies and ENISA via a self-disclosure and name possible vulnerabilities of their own. How-

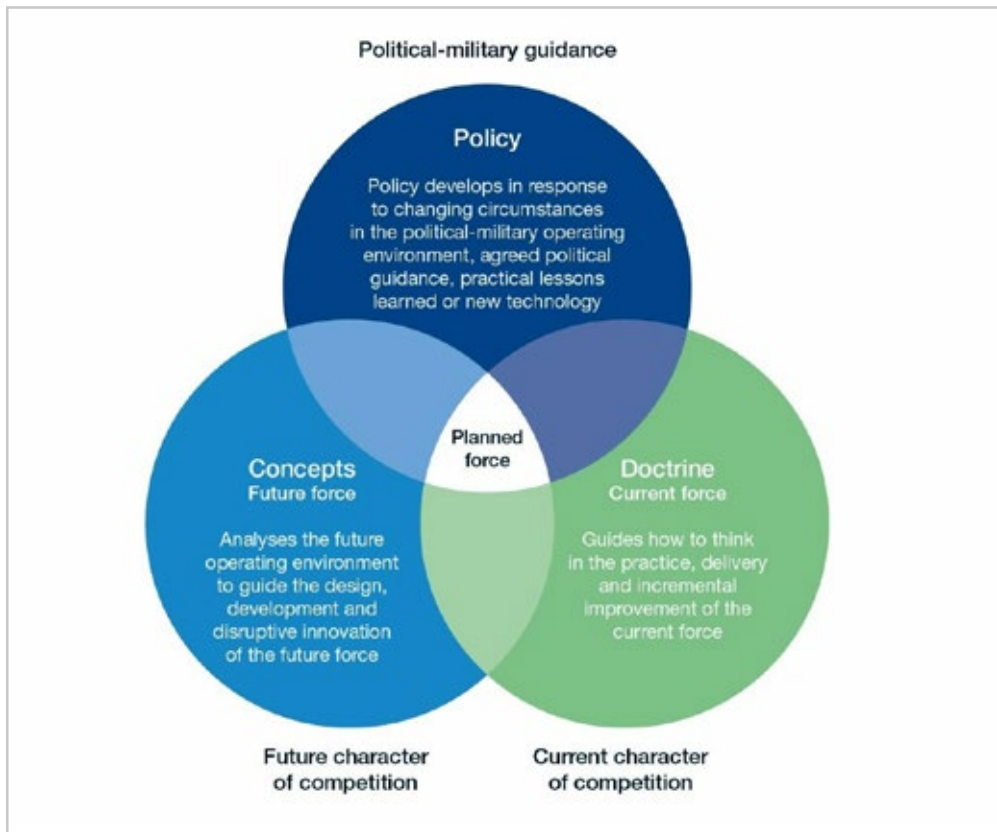


Figure 17: Planned acting is mediating between doctrine and new concepts as well as practical policy. (NATO STANDARD AJP-01(F))

ever, this approach is unfortunately a potential source of error in itself, because relying on the voluntariness of multinational corporations has already proven to be a mistake several times in the past.

International corporations such as Microsoft, Huawei, or Samsung are very reluctant to disclose their own software architectures. For instance, Microsoft’s Windows OS architecture is kept as a trade secret and not made available to the public<sup>30</sup> – it is not for nothing that so-called “reverse engineering”, in which the programming of a system is virtually cracked, is prohibited for commercial products by software giants<sup>31</sup>. This is a clear right of defense of the companies against the state and also against the competition, otherwise the intellectual property would be blatantly violated.

Nevertheless, it would be advisable, especially in the case of software applications, to strengthen the negative dynamic in such a way that independent control and verification of the products is made possible.

In order to achieve this, it is advisable to reduce the number of agencies, not to multiply them and to let them have overlapping responsibilities and duties. Here is an example:

“Many cooks spoil the broth” says a well-known proverb, and overlapping and competing structures are precisely the manifestation of this emblematic saying. There are already signs of conflict between ENISA and EC3 because of mismatched competencies in the area of criminal prosecution. ENISA does not have an executive mandate, which can only be given to the EC3 by EUROPOL, but since such institutions have investigative powers at the same time, a negative sense of competition could be created. This is further reinforced by the tendency of state and supranational bodies not to make findings from their own institution fully available, even if only in the context of administrative assistance, insofar as they concern the relevance of their own institution.

The EC3, in turn, violates in some respects the separation of intelligence and police powers, at least from a German constitutional point of view. Here, in turn, the general problem arises that these two areas cannot be clearly separated from one another in cyberspace. Multinational corporations, third-state actors (China, Russia, etc.), politically motivated activist organizations and their manifold hybrids (for example, Huawei as an international tech giant based in the People’s



Republic of China, Russia's "patriotic hackers") are difficult to monitor with purely police measures.

These kinds of problems with various interconnected particular dilemmas will be called chain problems in the further course. Efficient securitization is achieved by simplifying approaches and hierarchies as much as possible, while maintaining accountability and the rule of law. This means, in logical conclusion, that increasing the complexity of securitization achieves exactly the opposite of what it was intended to solve.

Any system with a certain number of elements will increase in complexity if additional elements are added. This means that the controllability of security-related events in cyberspace is reduced by a multiplication of parallel and competing control instances.

Another example of this dilemma is the Joint Cyber Unit, NIS cooperation group, and EU CyCLONe, all of which appear to be addressing the same issue: Better networking and cooperation between individual member states. Nevertheless, it is legitimate to ask why it is necessary to establish three structures that essentially do the same thing and possibly create a negative competitive relationship.

In addition, there is a questionable effectiveness of various EU institutions. EUINTCEN has already been mentioned in this report, this organization fails because the individual national intelligence services are often not willing to share their intelligence directly with all other services of the member states. They prefer direct exchange, and the EUINTCEN reports are largely of poor quality. In addition to the low added value for the member states, this institution has assumed the potential of an intelligence service of the European Commission.

Such, the solution is not to be found in more mushrooming of agencies, even though it might ease the need to become active somehow. The recipe for success is much more to reduce the number of institutions, to bundle, reassure and safeguard their competence and

***“European countries should not blindly adopt the American strategy of persistent engagement and defending forward, but they should move beyond the current standstill and design strategic frameworks as to how to prevent, discourage, and respond to continuous adversarial cyber behaviour short of war. This is crucial if they engage with the broader political and democratic difficulties related to increased strategic cyber competition.”***

Dr. Tobias Liebetrau, Postdoctoral researcher at Sciences Po Paris and the Danish Institute for International Studies

to make them responsible and accountable to the public. This ensures quality, trust and security. Unfortunately neither is currently the case.

This leads us to the next important remark: No legislation is always better than bad legislation. In some way one can compare it with poor software programming: Loopholes and flawed parts that cause harm have to be patched over the time and in the end a mixed up chaos is the result, which does not resemble anything that is of practical use to the people.

An example for such an abstracting dynamic which in this case is decidedly negative in the sense of a liberal-democratic basic order in Europe and concerns the area of cyber security and disinformation on the level of civil liberties. The Digital Service Act aims to better protect EU citizens from illegal content and also from disinformation. Nevertheless, it is not transparently regulated what is understood by the broad term of disinformation and to what extent so-called “content filters” on social networks can also lead to severe cuts in freedom of expression through the back door.

The EU Parliament has already complained several times that the EU Commission's strategy is to maintain a so-called stay-down rule for content in cases of doubt. In plain language, this means that in unclear circumstances, the Commission, or the bodies associated with it, reserve the right to censor the material without justification, or to place a rigid filter on it. This approach can severely damage the freedom of expression. Furthermore, the trust of citizens is also damaged when, on the one hand, data retention and warrantless searches of chats are considered, but on the other hand,

high-ranking officials, such as EU Commissioner von der Leyen, delete text messages from her official phone that are of interest to the public and refuse to provide clarification in any other way.

The DSA is bad legislation because it has no checks and balances, only a vague definition of hate speech, and presupposes the trust that the EU Commission will already know what should be banned and what should not. After all, it is the Commission that will interpret what is to be considered a prohibited expression of opinion and who should therefore be excluded from public digital discourse<sup>32</sup>. Big Tech in Social Media might with high probability react to this vague regulation with over-compensation: banning rigorously everything that could be maybe interpreted as hate

izen, and not as it should be: a defense for the citizen against an abusive state.

It is also unclear how the EU intends to apply its cyber-security strategy to so-called open source products. A considerable number of software developers, companies and private individuals rely on code that is freely accessible, but of course used at their own risk; after all, it was created through creative knowledge sharing and not for commercial reasons.

However, the Cyber Resilience Act stipulates that as soon as money is made with the code, i.e. it is used for commercial purposes, the regulations of the directive take effect. This would result in considerable additional costs for developers, who would suddenly have to cre-

*“The goal must be to strengthen the cooperation between civil organizations, the state, the EU and the citizens to fight online disinformation and cyber threats on a holistic basis.”*

Belén Carrasco Rodríguez, Project Director “Eyes on Russia”,  
Centre for Information Resilience



speech, in order to avoid penalties. Every law must be formulated and constructed in such a way that it can never be misused to establish a police state. This is not the case with the new DSA.

It is more than disturbing that the DSA, in conjunction with the German NetzDG, has already served as a blueprint for authoritarian states to adapt their legislation to more censorship, control and suppression of freedom of expression to the digital age. Russia, Venezuela, the Philippines and Malaysia even adopted roughly the same wording. There, too, the elastic, vague terms “hate speech,” “fake news,” and “propaganda” serve as justification for blocking millions of citizens from the Internet or deleting their accounts.

Much more than making the internet a safe space for online discourse and exchange of opinions, the EU Commission shows with the DSA an attitude that could be misinterpreted as deep distrust in the population – it is a defensive legislation for the state against the cit-

ate all the specifications for the security of a program that is actually freely available. Similarly, it is not clearly regulated when a newly developed software falls into a “high-risk” area of the regulation and when it does not, because modern applications have the characteristic of being able to be used for a wide range of different applications.

A strong restriction on this side could have the effect that only large software developers would be able to bear such costs, resulting in monopoly positions on the market. In cyberspace in particular, it is necessary to keep the market diversified and broad in order to reduce dependencies on third-state actors and to preserve citizens’ choices. Europe is not a forerunner when it comes to innovative, strong and leading software companies, it would be bad policy to create more obstacles for them to compete.

What about programs developed by private individuals who use them themselves or pass them on to friends

and acquaintances for private use? This is a question to which the new guidelines have not yet been able to provide an answer.

Ultimately, it is questionable whether the EU's new compendium of reforms and initiatives will really be able to increase and better protect cybersecurity in Europe, as well as deal with real disinformation. The Internet does not respect (supra-) national borders and the sources of insecurity are sometimes beyond the EU's control.

Server farms from which attacks on computers are launched are often located in countries of the global south, which have no capacity and rule of law to stop illegal actions from these computer systems. Although the new regulations and acts provide for better cooperation with these states, it is questionable how this can be implemented in a results-oriented manner. The West is currently in stark competition over influence in the Global South, and its competitors, foremost Russia and China, are massively expanding their presence in this region. The current, rather vague strategy of "strengthening cooperation" is too half-baked to actually achieve feasible and convincing results.

Another problematic aspect that illustrates well the character of the effectiveness of abstracting dynamics is the banning of media that are under the direct control of the Kremlin. Of course, disinformation and propaganda is spread there, this is beyond question. However, it is not certain that the banning of TV channels and blocking of Internet sites really had the desired effect.

The thinking of political decision-makers is still too much shaped by the assumptions of pre-digital times. Such "blocks" can be easily circumvented, even by inexperienced citizens: Through so-called VPN networks, which can be purchased quite legally and which simply cannot be banned because this would blatantly curtail the protection of individual privacy. Transparency International has repeatedly pointed out that the institutions, especially the EU Commission, have massive transparency deficits, which may correspond to internal regulations of "good practice", but must be considered absolutely insufficient in the area of independent control of the EC by the EU Parliament and other parts of the "checks and balances"<sup>33</sup>.

The blocking showed much more a mistrust of the political leadership of the EU and its member states in

the maturity of their citizens and their ability to weigh things up for themselves. To a large extent, it even achieved the opposite of what was actually intended. By blocking RT, for example, the site was given a certain legendary status and individual sections of the population gained the impression that a "truth was to be hidden from them." This is not a plea for unblocking, but should rather be understood as a lesson learned for future courses of action.

Similarly, as has already been mentioned, the same is true of social media. It is possible that the wrong lever is being used here, for example if Twitter is to be persuaded to take strict filtering measures. Not only have we seen that these companies can themselves have a bias in their political opinions, they can also develop a pattern of behavior that can be described as overcompliance – the preemptive and unreflective banning of any expression of opinion that even involves the suspicion of not being legal.

A reverse approach would be more advisable: defending citizens' essential right to free speech against these very companies and their desire to influence society. The distortive and manipulative behavior of big tech companies in the social media sphere has reinforced a dangerous trend that has already damaged the culture of debate in our liberal democratic order: polarization and tribalization. In short, citizens are forgetting to see themselves as an equal part of a discourse community and see dissenters as bitter opponents and enemies to be pushed out of the opinion space. This phenomenon now affects all political spectrums in all EU member states.

The "Fact Checker" initiatives within the EU have unfortunately also played their part in reinforcing this trend, but this will be discussed in more detail in the subchapter for Germany.

#### **Policy Recommendations:**

##### **■ No legislation is better than bad legislation**

Innovation and digital literacy will be the driving forces of the future. Educated citizens, who are aware of technical features, their functions, implications, usage and limits are the cornerstone of the new digital society. A climate of trust and security has to be established through unified and simple solution-oriented approaches.

Good legislation is not achieved through regulations that place every citizen and every company under sus-

pcion in advance. Good legislation is also formulated in such a way that it cannot be exploited to build a police state. Good legislation makes it possible for checks and balances to objectively monitor and apply the interpretation of a regulation. Good legislation reduces bureaucracy and sprawling, overlapping administrative procedures and allows citizens and businesses to develop on their own responsibility.

► **Many different sizes fit all**

There is no option to meet the needs of all participants (industry, civil society, etc.) in just one law (One size fits all). If done so, the result is full of loopholes, inconsistencies and problematic like in the current EU legislation concerning Internet issues. A better solution might be to tailor different regulations that addresses the diverse needs of all groups.

► **Legal Certainty**

Bad legislation has one of the most dangerous consequences: Uncertainty. Citizens, but as well businesses will reduce their activity or implement very restrictive terms of use, to avoid any collusion with the law and possible consequences. The result is a restricted internet culture, where should be an open and creative internet culture.

Stretchable terms like “Hate Speech” that lack consistency and definition rather cause uncertainty and distrust in the motives of the EC.

► **Regain trust through good practice in law and low compliance costs**

The internet is nothing that could be limited to a certain geographic space, it is a global, interconnected phenomenon. Laws should have in mind global practice and the needs of a globalized community. Business and intellectual exchange should be improved and not be hindered by poor and restrictive local legislation, that might render the EU unprogressive and uninteresting for investments, business and personal expression. Compliance costs should be minimized in order to attract and encourage businesses as well as citizens not to restrict themselves.

► **Keep it dynamic to keep pace with**

Legislation is often very slow, and renders itself obsolete in the moment it enters into force because the technological features it addresses have changed. Cyberspace is a dynamic and fluid phenomenon – legislation should keep that in mind and adapt swiftly. Online commerce sees new trends emerging within the blink of an eye, new services and new apps pop up every

week with new features – law has to have the competence to adapt

■ **No Mushrooming of new agencies**

Multiple parallel structures which might stand within an unhealthy relationship of competition do not solve problems, but produce more of them. “Hyperactivity” and the mushrooming of organizations and institutions might give a certain calming sense that “something is done”. Yet, in a crucial time, where Cybersecurity is at stake there is no room for such kind of action. The EU needs less agencies, but unified and clustered institutions that can act swiftly, direct and without long bureaucratic procedures. This might sound hard to accomplish, but it is necessary to fight Cybercrime, Cyber Espionage, Cyberattacks and Disinformation. Within the web things change fast and with the availability of Open Source Code, hackers for hire, and new emerging malicious software within the blink of an eye, there is simply no time for long bureaucratic multi-layer systems.

► Reduce the number of agencies that address Cybersecurity issues on the EU level to one unified institution, with exception of EC3

► Dissolve EU INTCEN for it is inefficient and often obstructive

► A new and unified, single Cybersecurity institution has to bundle, reassure and safeguard their competence and to make it effective, as well as responsible and accountable to the public

■ **Protection of innovative activity**

The strength of the European Union lies within its power for innovation and research. There should be no legislation that hinders new and fresh ideas when it comes to technological progress and development. Open Source should be under scrutiny, but it is no wise course of action to produce more costs for small and medium software development companies because they have to implement expensive security measures by themselves. Much more, the EU should make use of its massive buying power to take research in their own hands.

► Small and medium software development companies are the motor of European digital industries. They should benefit from tax exemptions to reduce costs, to keep the European market fit for international competition, as well to make the EU interesting for founders and investors.

► The EU should make use of its financial power and create software and innovation centers to ensure that it is on top edge of new development and innovation processes in the field. In terms of technology investment and innovation beats regulation

#### ■ Big Tech needs accountability not backdoors

However, it is not a good idea to authorize a single entity like the EC to demand lists from users, to prescribe content arbitrarily, and to ensure no accountability, neither from the EU, nor Big Tech. The backdoors in software systems that can be used by democratic states can also be used by totalitarian states to penetrate platforms and spy on users. Big tech companies have no problem with this because they think in terms of profit, not morality. Ericsson, for example, developed wiretap technology for Vodafone products and initially wanted to make it available only to states that demanded access. However, the tool was discovered and abused by hackers, because products without such backdoors are more secure than those that have them. Big tech must be subject to rigid accountability, transparency about its own practices, and responsibility.

#### ► Enhance transparency and accountability

Mandate increased transparency from Big Tech corporations regarding their algorithms, data practices, and content moderation policies to ensure they can be held accountable. This can help protect civil rights such as freedom of expression while curbing misinformation and discriminatory content.

#### ► Interoperability and Data Portability

Foster interoperability standards and data portability requirements to minimize vendor lock-in. This would enable users to easily switch between platforms and reduce the dominance of a single platform.

#### ► Public-Private Partnerships

Collaborate with tech companies to establish self-regulation mechanisms and industry standards that align with EU values and respect civil rights. This approach can encourage responsible behavior without excessive government intervention.

#### ► Implementing Stronger Antitrust Measures

Strengthen antitrust regulations to counteract anti-competitive behavior by Big Tech firms. This may involve stricter enforcement of existing laws and, potentially, the introduction of new legislation aimed at addressing digital monopolies.

## Sources and Further Readings:

**Stiftung Wissenschaft und Politik: Options for Enhancing the Flow of Information and Political Oversight.** 2018. By Raphael Bossong.



**Article 19: At a glance: Does the EU Digital Services Act protect freedom of expression?** February 11, 2021.



**European Court of Auditors: Challenges to effective EU cybersecurity policy.** Briefing Paper. 2019.



**Blog: Schneier on Security.** Bruce Schneier, Fellow of the Berkman Center for Internet & Society and Lecturer in Public Policy at Harvard Kennedy School



**Stiftung Neue Verantwortung e.V.: Response to the European Commission's Consultation on Digital Services Act (DSA) transparency database.** July 11, 2023. By Martin Degeling, Anna-Katharina Meßmer, Julian Jaurisch.



**Guardint: Researching Surveillance, Intelligence & Oversight**



## B. NATO – backup for the worst case

The North Atlantic Treaty Organization's efforts and initiatives are comprehensive and impressive. It is in the nature of things that current projects and plans are subject to a level of secrecy. It follows that the current maneuvers and structures are already "old", not in the sense of "out of date" but they are established standards and will be further developed.

NATO is more innovative, direct and modern in terms of direct implementation and adaptation to alliance defense – but it also less of a complex political structure than (supra-) national entities such as Germany or the EU. However, it shows that NATO will be able to stand up to antagonistic forces such as Russia and China in the area of military defense and securing critical infrastructure in cyberspace.

This is the result of, among other things, the establishment of StratCom and Cyber Command in Latvia, working groups with strategies for cyber defense and constant evaluation by the individual, participating units of the armies of the member states.

Despite all this, however, NATO also has a few weaknesses that should be addressed at this point.

The Internet of Things in general is already a worrying development. After all, it is not obvious what the need is to connect a refrigerator to the Internet. However, it is even less comprehensible why entire radar stations should be linked to the network. Again, this linkage creates interlinked problems.

Digitization is an irreversible process, there is no way to turn back the wheel of this development and there is no interest in doing so. This is because all international players are striving to gain an advantage over each other, including in cyberspace. The trend is clear, even NATO is striving to develop more and more Joint All Command and Control Systems (JADC), i.e. capabilities, effective military communications of all agencies via digital means.

However, there is nothing to be said against this, and it also seems advisable to keep analog backup systems in reserve to counter any malfunctions or sabotage through hacking with protection and resilience. In concrete terms, this means that analog systems that are off-grid are actively replaced, but are still kept functional as a reserve and back-up.

This applies to conventional encrypted radio communication, autonomous and manual control of critical infrastructure and much more.

If a NATO facility were to be crippled by a cyberattack, which protocol and which rapid support unit would be deployed, in which location, and how? If it turns out to be a planned action, on the part of a foreign state (China, Russia) how will NATO respond? Would this be a case for Article 5 of the Act of Alliance? After all, the Alliance has affirmed that a cyber attack could also constitute an armed attack.

But the question is how to respond to that attack and what the consequences might be. Again, thinking is still too much shaped by pre-digital times and the legal framework has not been adapted to modern developments. The way to react to a cyber attack is a counter-attack – in the field of the Internet, this is also referred to as a hackback. Considerations of this approach can also be found in the European Union, among others.

However, it is not clear how such an attack should be carried out and to which targets it should be limited. Assuming that a hacker attack on one of the alliance countries would have caused some damage in the area of data, but would not have led to any material or human losses. It is a complicated question to what extent this is already an act of war and what counter-measures are taken in response without getting directly into an armed confrontation. Most of the states that have relevant and powerful cyber units are themselves nuclear powers, first and foremost Russia, China and India. Many considerations currently exist on the abstracting dynamics side, such as the hackbacks mentioned above, but there are no progressive dynamics such as efforts to develop a functioning cyber diplomacy to prevent the escalation of a cyber-level exchange of blows from potentiating into a potential world war.

Meanwhile, however, all sides-NATO, China, Russia, and in all likelihood India-are building up capabilities for so-called cyber first and second strikes, much along the lines of nuclear first and second strike capabilities during the Cold War. These focus primarily on the critical infrastructure of the respective adversary in order to collapse the respective societies. This means that in addition to the nuclear "balance of terror," or Mutual Assured Destruction," a "balance of cyber terror" is being established, further deepening and exacerbating the complexity of the security network across the globe.

*“...the EU is neither the only nor the primary international organization which seeks to gather a powerful role in the global governance of the internet.*

*Most crucially, there is not only the International Telecommunications Union (ITU), but NATO and its Cooperative Cyber Defence Centre of Excellence in Tallin. Similar to the situation in conventional security, NATO does not have a genuine interest to let the EU grow in this policy field and to gain something close to strategic autonomy. Normally, it prefers something closer to strategic cooperation or even dependence.”*

Dr. Moritz Weiss, professor for International Relations  
at the LMU University of Munich

At the same time, there is an ever-increasing overlap of civilian cyberinfrastructure that can be harnessed for military use. A good example of this is represented by the current innovations of the Ukrainian armed forces in the field of digital warfare. For example, a kind of “Uber”-style app has been developed in the field of artillery coordination. Russian soldiers were trapped via the dating app Tinder. Civilians were urged to find out the distance of enemy soldiers who are active on the platform (this is automatically displayed) and pass it on to the armed forces.

Here we move toward a new dilemma: the blurring of the lines between civilian and military technology in the digital realm and a merging of the offline and online worlds. Various countries are familiar with the model of “total defense” in the event of an attack, that is, the involvement of the civilian population in defensive measures. However, many other countries do not know this principle and try not to make their population a target.

Do the civilians who help the armed forces on Tinder, for example, become combatants? Can companies that develop apps, for what are actually civilian uses, become military targets? These are questions that remain unanswered to this day.

Another point for constructive criticism that should not go unmentioned here is the detriment of internal friction within the NATO alliance. Most of the member states of the EU are at the same time also in NATO, in

spite of everything the EU also tries to coordinate the continental European defense more effectively between the countries. The PESCO model mentioned in this report is just one of them, there are others such as the EU Battlegroups.

In recent years, however, there has been massive lobbying, especially by U.S. defense contractors and individual members of Congress, to prevent the PESCO project. The fear is that a coordinated pan-European approach would cause a loss of income for defense companies and weaken U.S. influence in Europe<sup>34</sup>. However, it must be emphasized here that this type of attempted influence does not strengthen Europe’s defense capability, but rather undermines it. A communication to Washington that the alliance must demonstrate unity and unity and that the security of a strong Europe also means the security of the USA would be necessary. Finally, there are neutral countries in the EU, as well as among the candidate countries, that are more difficult to integrate into a defense architecture, especially in a sensitive area such as cybersecurity, because of such processes.

#### **Policy Recommendations:**

##### **■ Keep analogue systems as crisis backup**

As already mentioned, digitization is irreversible and a trend that will continue, especially in the field of Joint All Command and Control Systems (JADC). Nevertheless, it is advisable not to completely dismantle the “obsolete” systems. Analog radio communications and manual controls, such as radar systems, are important

as backups and can be easily reactivated in the event of a hacker attack, or even an EMP strike, or even a solar storm.

► Even though modernization, that is digitalization proceeds and is inevitable, “old” forms of defense communications and reconnaissance technology should be kept maintained and ready

► It is wise to invest time and assets in teaching young military personnel in the usage of the “obsolete” technology, in order to have it up and ready in any case

■ **Keep Nuclear Weapons strictly off the grid**

Despite some criticism that modern technology did not transpire to the realm of Nuclear Deterrence, it is highly advisable that it never will. The effects of a hacking, which can not be excluded with all certainty if the control and launch devices are connected with the net, would be devastating. Currently, all these systems are absolutely unhackable and it is wise to keep them so.

► All systems for command, control, aiming, launching and service of nuclear weapons has to be kept off the digital grid at all costs

■ **Develop Cyber Diplomacy**

Developing countermeasures and reactions to Cyber-threats is important and should remain the first task of NATO as a defensive alliance. Still, technological progress and competence building should not be the only course of action. We live in volatile times and confrontations between Great Powers could, again, not be excluded. In order to avoid a spiral of escalation, Cyber diplomatic capabilities should be developed, enforced and implemented to settle possible conflicts at the negotiation table.

► Establish a “Red Smartphone”  
In analogy to the “Red Telephone” from the Cold War between Washington and Moscow there should be a fast lane for crisis communication between the major international blocks of power concerning cybersecurity issues, especially cyberattacks.

■ **Unity is strength**

During unstable times in International Relations, there should be no place for internal divisions and skirmishes. Lobbying against EU efforts to strengthen its abilities to defend should not take place and should be as well strongly discouraged. Defense and security of

the entire continent are simply no place for lobbying out of profit reasons, especially not in the sphere of Cybersecurity where unity of the entire alliance tightly coordinated with the EU is more necessary than ever.

► **Cooperation not competition**

EU and NATO are quite different. While the EU is a supranational body based on shared values, NATO is an intergovernmental organization based on a common interest, which is defense. Still, most of the countries that are members of both share the same values, interests and communalities. There should be an agreement, that both bodies do not work against each other, this would diminish trust and such joint ventures.

■ **Counter Disinformation with public awareness and openness to criticism**

Show that NATO is not what its adversaries is: An alliance of free nations ready to defend its populations, states and values. Further, convert into a strength, what is perceived by authoritarian states as weakness: Openness to constructive criticism. As we learned, disseminated disinformation often carries a core that is not entirely untrue, but warped, misplaced and decontextualized. Play with open cards, acknowledge mistakes, address doubts and present your current and constant commitment to improve and transparency. Denial is the wrong reaction to disinformation, discussion and synergy with criticism is what the greatest strength of NATO has to be.

► Meet cognitive warfare methods like psyops and disruption with rebuilding trust among the civilian population. Seek out direct contact with citizens and their questions, treat the population as partners and allies in a collective readiness to defend freedom and democracy.



## Sources and further readings:

**The German Marshall Fund of the United States: EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions. 2017.**  
By Bruno L  t   and Piret Pernik.



**POLITICO: NATO prepares for cyber war. March 12, 2022.** By Maggie Miller.



**Council on Foreign Relations: Why We Are Unconvinced NATO’s Cyber Policy Is More Aggressive, and That’s a Good Thing. February 06, 2018.**  
By Daniel Moore, PhD.



**Chatham House: Cyber Insurance for Civil Nuclear Facilities – Risks and Opportunities. May 08, 2019.**  
By   ireann Leverett.



## C. Germany – ad odds with itself

The German concept of a cyber strategy is one thing above all: typically German. Detailed, with precise ideas and division of tasks. However, does the “situation on the ground” correspond to the assumptions, expectations and design options from the individual ministries and the federal government?

Unfortunately, Germany is not a “world champion” in the area of digitization, as it is in the case of goods exports, for example. The Digital Economy and Society Index (DESI) published each year by the European Commission, which surveys the progress of member states in the five key areas of connectivity, digital skills, Internet use by private individuals, integration of digital technology by companies and digital public services, places Germany only in midfield. (Ranked 13th out of 28)

German companies were hit hard by the Corona crisis and its restrictions, as well as by the economic effects of the associated financial crisis and the Ukraine war. This also affects the field of digitalization of the German economy and also includes gaps within cyber security. But progress does not wait, and internationally, of course, antagonistic forces are continuously improving their capabilities – and threatening to leave Germany behind in the process.

At first glance, this may not seem particularly disconcerting, for example, if only a small portion of public administration is digitized at all. At the end of 2022, out of a possible 575 administrative files, only 50 were possible digitally, the rest are still only possible in writing, and many German authorities still use the antiquated fax machine. Of course, this has the advantage that it is difficult for hackers to penetrate this type of administration, but it is not up to date and threatens to fall behind in European comparison.

The economy and citizens are dependent on up-to-date, fast, uncomplicated and reliably functioning administrative acts. It is urgently necessary to build up these capacities, but at the same time to provide sufficient security for this type of modern administration. This is a paradoxical situation and part of a larger complex, which the French philosopher Paul Virilio also called “frenzied stagnation” and which would primarily affect Western countries.

A lot is planned, suggested and started, but comparatively little or nothing is implemented. The result is a chaotization of everyday life, which also has an unsettling effect on the population and the business climate.

It would therefore be important and necessary to streamline bureaucracy and strengthen the progressive dynamics of digital literacy and awareness among citizens in the area of digitalization and its securitization. After all, cybersecurity starts with people and their knowledge of how to use modern technologies and only ends with the operation and technical properties of the devices.

In the fight against disinformation, the German government is also relying primarily on abstracting

filter bubbles on social media and the blanket application of the term “conspiracy theory” to everything that is not immediately one hundred percent provable has hardened the fronts of discourse and made it difficult to exchange opinions.

Arguments are rarely exchanged on Twitter either; much more, especially in German-speaking countries, ideological battles are waged there with extreme bitterness and harshness – if those involved communicate with each other at all and not just in their own “bubble,” as it is called today. Of course, hate and incitement are a problem on the Internet, but the question is whether restrictive measures in the form of criminal laws are really effective, even capture the problem, and whether they have even been sufficiently

*“Here ways have to be found to adapt to the threat level while ensuring constitutionality of the system, avoiding that a policy done in one area causes more damage in another. Further, that measures taken without being synergized or well thought through just go without impact.”*

Julia Schuetze, M.A., Cybersecurity Policy and Resilience Project Manager, Stiftung Neue Verantwortung e.V.



dynamics, such as the new Section 188 of the German Criminal Code (StGB), which, contrary to widespread assumptions, is primarily intended to combat so-called fake news and disinformation. It provides that insults to the honor of politicians will be punished if they serve to impair the reputation and work of the functionary. As is typical with criminal laws, it has a restrictive character and is unfortunately also not sufficiently defined. When the scope of laws is expanded, the questionable areas of these regulations are automatically massively expanded as well.

For example, if an online journalist, citing an anonymous source, publishes an article and promotes on Twitter that there is a suspicion of corruption among a certain mayor, the latter could file a complaint under §188 StGB.

This kind of approach unfortunately reflects the widespread tribalization of society. The echo chambers and

defined. Not every pointed statement on the net is immediately hate speech, and there is little nuance in distinguishing between irony, satire and emotional affect. “Hate” in this sense is also difficult to ban; after all, it is a human emotion whose reasons lie deeper and which is just as difficult to sanction by law as, say, “love” in reverse. How exactly is “hate speech” defined finally? It is a matter of highly subjective and even emotion-based assessments. A pointed and critical speech in the Bundestag can be perceived as “hate” by some, and this is also the case with certain tweets, for example. However, the law must not take subjective feelings as a basis, but must use objective criteria. This is currently not the case enough.

As we have already learned, Russian and also Chinese disinformation is not trying to create new opinion, an undertaking that would be far too complicated. It seeks to reinforce and deepen already existing social fault

lines. Unfortunately, it must be noted that the social networks have strengthened this trend with their own, often politically colored, filter and shadow ban mechanisms, i.e., in a way they have unconsciously followed the Kremlin's methods.

When certain opinions and theses are simply forced out of public discourse, this leads to uncertainty and dislocation among people. Evasive behavior develops, which can be easily implemented on the Net. Following a lockout from Twitter, Facebook and the like, citizens move to other platforms, where more radical and closed world views sometimes prevail. A good example of this is Telegram, a network that is largely unmoderated and on which radicalization can very easily take place.

Unfortunately, the so-called "fact checkers" have also done the fight against disinformation and fake news a disservice so far, rather than leading to a relaxation and reintegration. Sites such as "Correctiv" have unfortunately been implicated in accusations of bias themselves, and court cases have found that untrue claims had sometimes been made<sup>35</sup>. The general problem with fact checkers lies in three reasons:

1. A misconception of science. Empirical science is not understood as a process in which new findings are made subject to possible falsification, but as a dogmatic process. There is an urgent need to train journalists in fact checking about basic scientific methodology and epistemology. The misrepresentation of research results as "incontrovertible truth" about which there should be no further discussion has led to confusion, especially in the times of the coronavirus pandemic, which was detrimental to constructive discourse.

2. A problematic understanding of the term "truth". Each person makes judgments based on his or her own knowledge and information. There is hardly such a thing as one hundred percent truth, as frightening as this may seem to many citizens. There are many shades of gray, yet a picture is drawn in which there is only "black" and "white" (which is also a result of the ideologically hardened culture of discussion on social media) and dissenters are no longer seen as debate partners, but are labeled "liars" and sometimes "mis-anthropes". (See the Streeck – Böhmermann debate<sup>36</sup>).

Fact checkers themselves have a problem with the objectivity of their work; they engage in so-called

"cherry picking," i.e., they cite primarily sources that underscore their own view of a certain phenomenon.

This reinforces polarization within society, because the respective citizens with a different opinion are perceived as "enemies" who are up to no good. This is also, by the way, the goal of Russian disinformation, exactly this effect is supposed to occur and the question must be asked to what extent our society has unfortunately fallen into the trap of the disinformation strategies of third countries precisely through its own measures.

Abstracting measures are of little help in the face of more fake news and more disinformation; there are plenty of ways to circumvent blocks and restrictions on the Internet. This begins with Telegram, but continues through other channels and extends into the dark web, which is only a few clicks away.

There should be much more plurality of opinion and debate again, also in the media, because the most powerful weapon against disinformation lies in the basic idea of our liberal democracy itself: Discussion and exchange. For if, for example, erroneous assumptions have to face an open debate, they very quickly and easily lose their thrust. What is needed is more trust in citizens and encouragement to exchange opinions.

According to a recent survey, two thirds of all German citizens surveyed think that the possibility of free expression of opinion is no longer fully guaranteed in every occasion<sup>37</sup>. This means that there is fear and withdrawal among people, the ideal breeding ground for radicalization and division. This also hinders constructive debate at the academic level. A good example directly related to cyberattack threat mitigation is the threat of a foreign-caused blackout in the power supply. In Germany, this debate has been framed by fact checkers and also various media into the realm of conspiracy legends and linked to right-wing extremist narratives. This is a strange circumstance, since in other European countries this danger is discussed quite openly and measures are taken to avert it. A good example is Austria, where the government and its ministries down to the municipal level are making preparations to avert such an existentially threatening scenario.

This illustrates very well that a return to a pragmatic and debate-based culture of discussion is more than urgently needed in Germany, especially on the Net.

*“For breached critical live production systems, there will always be an aspect of having a balance between downtime and service/production losses when securing vital evidence.”*

Johnny Bengtsson, Forensic expert,  
Swedish National Forensic Centre (NFC)



### Policy Recommendations:

#### ■ Accelerate digitalization

The current progress of digitalization in Germany is simply not satisfying. In the current speed, it might take years, if not a whole decade to accomplish an operational digitalization of just the most basic administrative acts. This means, that there will still happen mistakes and hardships along the way that might even more obstruct the process and delay an effective securitization of the issue. In the end a chaotic situation could be created, which would disconnect Germany as a country from an ever faster progressing world.

► There is no excuse for black spots on the map  
In some regions in Germany there is still neither a reliable internet connection nor network reception. This slows the country down in its economic, academic and civil development

#### ■ Improve digital literacy of the general population

Most of the citizens in Germany already use computers, IoT devices, smartphones or other technical products that are connected to the internet. Still there is a stunningly low level of knowledge within the society about the functions, implications, applications, dangers and possibilities of these devices. The school system has to be reformed in a way, that pupils do not learn to handle these products alone and by themselves. Such an approach would always be piecemeal, incomplete and a source of danger.

Still digital literacy encompasses far more than simple technical issues. It is the ability to act autonomous and enlightened in a digital world. This means as well, that citizens can examine information in a critical and autonomous way. Awareness has to be built, that not

every information in the net is equal and trustworthy, and that it is necessary to reflect material in a objective manner in the net.

Only about 2% of all hacked databases are the ones of large institutions, or companies. The vast majority are private computers, that are for good reason not under state scrutiny, but in the responsibility of each private user. Verizon's Data Breach Report 2022 reveals that insiders have caused 20% of global data breaches.

► Use state funds to make schools nutrient soil for cyber resilience

Basic, mid and higher education have to integrate mandatory courses in internet privacy, security and good practice. Community colleges have to increase their offer in effective courses for internet security and data handling.

#### ■ Stop Big Brother in its wake – Make governmental bodies independent and accountable

The BSI is an important agency, but it should be quite independent from the Ministry of Interior Affairs. There is the possibility that security gaps remain unaddressed by order of the Ministry for exploitation by the intelligence services. An independent BSI can serve the needs of the citizens, the state and business way more efficient and reliable. It creates as well trust and security, which is the main reason it should exist in the first place.

► Responsible Disclosure

It has to be mandatory for the BSI to report security gaps and detected backdoors immediately and transparent. All participants and stakeholders in the internet can work then on a solution to fix it.

- ▶ Take advantage of the swarm...

Responsible disclosure can activate the entire internet community to work on a solution for a certain security gap.

- ▶ ...but hold the developer responsible

Software companies should be obliged to fix security breaches in their code. If necessary, even punishable with a fine to ensure compliance.

■ **Use Open Source code for critical infrastructure**

Imagine you have a digital security system, but the company that manufactured ceases to make business. It would be very hard to retrieve the code and to access it, legal problems might as well delay an adequate and swift reaction to a breach. This is why good security code is based on Open Source technology.

- ▶ Keep it stored

Open Source solutions can be stored by institutions in order to have them ready to create a fast solution

- ▶ Enable the Federal Agency for Technical Relief (THW) to have the capacities to aid in digital cases of emergency, this would ensure a reliable, unbureaucratic and swift reaction to security breaches. The digital sphere is just another part of critical civilian infrastructure, and such it should be taken care of by well organized professionals that are financed by the public

■ **Constructive dialogue, transparency and openness for debate instead of biased fact checking**

- ▶ Like in the recommendation for NATO, it is crucial to expose own mistakes and work on improving the situation. Disinformation loses its own scandalous and disrupting edge if it is shown, that there might be sometimes a true fact in it, just depicted in a very distorted way. It is no shame to speak about own failures, it is a shame trying to cover them up

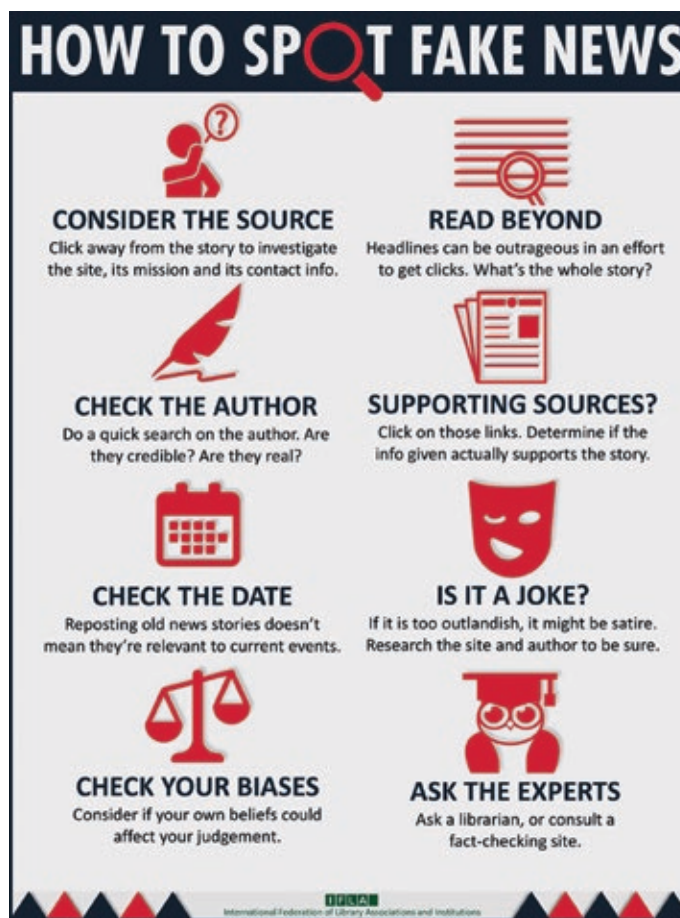


Figure 18: Dealing with Fake News might not be an easy task. Courtesy of Cornell University. Courtesy of FactCheck.org

## Sources and Further Readings:

**Stiftung Neue Verantwortung e.V.: Germany's Cybersecurity Architecture. April 2021. By Rebecca Beigel & Dr. Sven Herpig.**



**AG Kritis: Political Demands. In German.**



**The New York Times: Germany Adopts a More Muscular Security Plan. Critics Call It 'Weak.' June 14, 2023. By Steven Erlanger and Christopher F. Schuetze.**



**Harvard Kennedy School: The presence of unexpected biases in online fact-checking. January 27, 2021. By Sungkyu Park, Jaimie Yejean Park, Jeong-Han Kang, Meeyoung Cha.**



## D. Global level – towards global online security governance?

The fall of the Iron Curtain, the dissolution of the Soviet Union and the Warsaw Pact did not lead to an “end of history” as Francis Fukuyama described it in the 1990s. Even he had to revise his theses in the face of the developments that followed. This is also true of the cyber realm which has developed in parallel to the post-1990 world order. There is a major need to address issues of tackling online disinformation and cyber insecurities on the international level, including international law.

This must be done without giving up the freedom of the Internet, the idea with which it was associated. Is it still the nation state alone that controls the destiny of this world? Yes and no. Multinational corporations have become powerful structures that are no longer limited to creating products and marketing them. Companies like Google, Microsoft, Apple, Twitter, Facebook, and TikTok sell more than mere software applications; they sell entire worldviews and ideas. This is a novelty that has not been seen before in this form. The question arises, however, as to whether the nation state, which still represents the creative power of human coexistence par excellence, even in times of globalization, should tolerate this competitive relationship.

Noam Chomsky has described corporations as the most perfectly totalitarian structures that man has ever created in his history. At that time, he was still talking about banks and industrial giants, but in the online sphere we are dealing with companies that also represent very specific views and images of humanity, and in which there is no internal discussion of this at all. This is a dangerous further development to his observation.

This development and interlocking may not be worthy of further notice in an authoritarian state, as is the case with TikTok, for example. It is not surprising that the Chinese-led company controls exactly what content it distributes where and for what purpose. However, it is troubling and alarming for democratic societies when companies that are not internally democratically organized set out to directly intervene in public discourse.

How to proceed in this respect is a question of state-theoretical and practical political nature, which in turn has to be solved multilaterally, since the companies in question also act on an international basis. Citizens will also be challenged, and digital literacy is

*“Somewhere there must be a starting point in multilateral and multidisciplinary cooperations to make cyberspace a safer environment. There is no better time than now and no better place than here.”*

Gazmend Huskaj, Head of Cyber Security,  
Geneva Centre for Security Policy



an absolute must in order to secure the future of democracy. Too much emphasis has been placed on restrictive measures, when the source of all democratic action is the individual. It is natural to be afraid of dangers, yet fear of change, also and especially through the digital, is not advisable and leads to irrational decisions. New trust must be created and a firm grasp of the freedoms and obligations in the online space must be instilled in our fellow citizens at school in order to shape the future.

However, paternalism and rampant regulatory hyperactivity are of little help if promoting people as rational and responsible beings in a democracy is the key to a holistic solution.

Willy Brand once said, “We want to dare more democracy,” and Konrad Adenauer’s saying, “No experiments!” has been handed down.

The solution to today’s problem of the phenomenon of cyberspace and (dis)information could consist of a synthesis:

Developing more trust in democracy without dangerous experiments.

#### **Policy Recommendations:**

##### **■ If we want a rule-based international order we have to live it**

The category of an international rule-based order will always remain to be a void category, if the participants are not willing to cooperate. Sanctions and containing measures against wrongful behavior is important, but there must be also incentives for sticking to rules and positive sanctions for those who have good practice on this field. There must be a sense for the digital world as if it is physical present, creating a world in which geo-

graphic borders are still there but in which online every state borders the other. Germany is in the web a direct neighbor country to Egypt, just as is Japan a direct neighbor of Argentina. No one is an island. There should be an international commitment to re-establish contact and working groups. The logic of “one nation prevails over the other and subjugates it” has to be diminished and replaced by a sense for the brotherhood of all mankind. As idealistic as it might sound.

##### **■ Create a “Red Smartphone” for all great powers in a new multipolar world**

As we mentioned the “red telephone” between Washington and Moscow that was established after the Cuban Missile Crisis in 1962, there should be a similar initiative in regard of the growing “race for cyber armament”. An anarchic system with cocked guns and no established diplomatic channels is a recipe for disaster. This is why all efforts should be taken to create rapid action diplomatic contact groups that could be activated to settle conflicts and problems first at the negotiation table.

## ODISCYE TEAM

**Prof. Dr. Stephan Stetter**  
Head of the Project  
Professor for International Relations and Conflict Studies  
University of the Bundeswehr Munich

**Lucas Maximilian Schubert, M.A.**  
Research Associate  
University of the Bundeswehr Munich

### We would like to express our special thanks to

#### **Bundeswehr Center for Public Affairs (ZInfoABw) and partners in Munich**

**Captain Christian Dienst**

**Dr. Jörg Jacobs**

**Maja Henke-Lloyd**

**Dr. Philip Jan Schaefer**

**Mustafa Isik**  
IT Consultant and Computer Journalist

#### **Participants of the ODISCYE Workshop**

**Dr. Vladimir Ajzenhamer**  
Professor on International Relations  
Faculty of Security Studies -University of Belgrade

**Dr. Annegret Bendiek**  
Deputy Head of the EU/Europe Research Group  
SWP Berlin

**Johnny Bengtsson**  
Forensic Expert  
Swedish National Forensic Centre

**Dr. Rolf Fredheim**  
Director  
Markolo Research

**Prof. Dr. Georg Groh**  
Computer Scientist  
Technical University of Munich

**Dr. Sandro Gaycken**  
Founder & Co-CEO  
Monarch IT Services and IT Consulting

**Prof. Dr. Florian Gallwitz**  
Computer Scientist  
Nuremberg Institute of Technology

**Prof. Dr. Anita Gohdes**  
Professor of International and Cyber Security  
Hertie School

**Dr. Christian Grimme**  
Computer Scientist  
WWU Münster

**Dr. Gazmend Huskaj**  
Head of Cyber Security  
Geneva Centre for Cyber Security

**Dr. Ross King**  
Computer Scientist  
Austrian Institute of Technology

**Lieutenant Colonel Lars Koreman**  
Bundeswehr  
SHAPE DEU NMR

**Dr. Tobias Liebetrau**  
Postdoctoral Researcher on International Cybersecurity  
Sciences Po

**Dr. Linda Monsees**  
Researcher at the Center for Governance  
of Emerging Technologies  
Institute of International Relations Prague

**Prof. Dr. Florian Muhle**  
Researcher on Digital Communication  
Zeppelin Universität Friedrichshafen

**Lieutenant Colonel Dr. Sönke Niedringhaus**  
Bundeswehr  
NATO StratCom

**Dipl.-Inf. Thomas Reinhold**  
Research Associate  
PEASEC, Technical University of Darmstadt

**Andrea García Rodríguez**  
Lead Digital Policy Analyst  
European Policy Centre

**Belén Carrasco Rodriguez**  
Project Director – Eyes on Russia  
Centre for Information Resilience

**Julia Schuetze, M.A.**  
Project Director for Cybersecurity Policy and Resilience  
Foundation New Responsibility

**Dr. Tim Stevens**  
Head of the King's Cyber Security Research Group  
King's College London

**Dr. Moritz Weiss**  
Senior lecturer in International Relations  
Geschwister-Scholl-Institute, LMU Munich

**Dr. Christopher Whyte**  
Assistant professor of homeland security and emergency  
preparedness  
Virginia Commonwealth University

**Tiffany Wong, M.A.**  
Director, China Practice  
Albright Stonebridge Group



### Special Consultants and Reviewers

**Michael Kreil**  
Data and Tech Journalist

**Prof. Dr. Jan-Hendrik Passoth**  
Head of the European New School of Digital Studies  
(ENS)  
European University Viadrina

**Colonel Dr. Markus Reisner**  
Theresian Military Academy Wiener Neustadt  
Bundesheer, Austria

**Univ.-Prof. Dr. Oliver Rose**  
Computer Scientist  
University of the Bundeswehr Munich

**PD Dr. Frank Sauer**  
Senior Research Fellow for International Politics  
University of the Bundeswehr Munich

**Marcel Schliebs**  
Political Data Scientist  
Oxford Internet Institute

### Bundeswehr Cyber Innovation Hub

**Sven Weizenegger**

**Lisa Zill, M.Sc.**

### Logistics, Planning and Administration

**Jheryl Dalugdog**  
Administration  
University of the Bundeswehr Munich

**Charalampos Karpouchtsis, M.A.**  
Research Associate  
Helmut-Schmidt-University of the Bundeswehr Hamburg

**Master Sergeant Kilian Östreicher**  
Student Assistant  
University of the Bundeswehr Munich

### Layout and Graphic Design

**allegria design**  
**Jutta Oppermann**  
Taufkirchen, Munich  
[www.allegriadesign.de](http://www.allegriadesign.de)

## FOOTNOTES

### Footnotes:

1. APnews: The superspreaders behind top COVID-19 conspiracy theories. February 15, 2021. By David Klepper, Farnoush Amiri and Beatrice Dupuy.
2. BBC.com: Putin's mysterious Facebook 'superfans' on a mission. April 11, 2022. By Jack Goodman & Olga Robinson.
3. Kotaku: 'Ghost Of Kyiv' Fighter Pilot Blowing Up Russian Aircraft In Trending Clip Actually From Video Game. February 26, 2022. By Ethan Gach.
4. Forbes: The Story Behind The Stuxnet Virus. October 7, 2010. By Bruce Schneier.
5. Cybersecurityhelp.cz: Fancy Bear APT strikes with a new spearfishing campaign, improves its arsenal to avoid detection. September 25, 2019.
6. Heise.de: Machtfrage. (In German: Power Question) February 13, 2010. By Monika Ermert.
7. Oberlo.com: How many people shop online?
8. Statewatch.org: US letter from Bush with demands for EU cooperation.
9. Bundesverfassungsgericht: BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 15. Februar 2023 - 1 BvR 141/16 -, Rn. 1-17. (In German)
10. § 100b – Strafprozeßordnung (StPO)
11. APnews: Rights group verifies Polish senator was hacked with spyware. January 06, 2022. By Vanessa Gera.
12. Deutsche Welle: Hungary admits to using Pegasus spyware. November 04, 2021. By ar/nm (AFP, AP).
13. Tagesschau.de: Bundesnachrichtendienst spitzelt mit Pegasus. (In German: Federal Intelligence Service spies with Pegasus). October 08, 2021. By Florian Flade und Georg Mascolo.
14. Getastra.com: Security Audit. 90+ Cyber Crime Statistics 2023: Cost, Industries & Trends. August 04, 2023. By Nivedita James.
15. TheRecord: Major German energy supplier hit by cyberattack. October 27, 2022. Alexander Martin.
16. Gridradar.net: Sagging of the UCTE mains frequency to 49.84 HZ. March 31, 2023.
17. Statista.com: Value of European Union exports to China in 2022, by commodity category (in billion euros).
18. "Наши" translates to "Ours!" a self-proclaimed anti-fascist youth organization that was one of the pawn groups of the Putin administration. Founded in 2005 and disbanded in 2013.
19. DemandSage.com: Twitter Statistics In 2023 — (Facts After "X" Rebranding). August 10, 2023. By Rohit Shewale
20. TheGuardian.com: How do you stop fake news about Covid? Not by silencing scientists who ask difficult questions. March 29, 2022. By Zoe Williams.
21. American Institute for Economic Research (AIER): Twitter Censors Famed Epidemiologist Martin Kulldorff. March 29, 2021. By Jeffrey A. Tucker.
22. digital-strategy.ec.europa.eu: The Digital Europe Programme.
23. research-and-innovation.ec.europa.eu: Horizon Europe
24. commission.europa.eu: Recovery plan for Europe
25. commission.europa.eu: The Recovery and Resilience Facility
26. Reuters: AI threatens humanity's future, 61% of Americans say: Reuters/Ipsos poll. May 17, 2023. By Anna Tong.
27. Zippia: 23+ ARTIFICIAL INTELLIGENCE AND JOB LOSS STATISTICS [2023]: HOW JOB AUTOMATION IMPACTS THE WORKFORCE. June 11, 2023. By Chris Kalmar.
28. U.S. Government Accountability Office: Artificial Intelligence's Use and Rapid Growth Highlight Its Possibilities and Perils. September 06, 2023.
29. Institute for Development of Freedom of Information (IDFI): How Russian disinformation tactics were utilized in the context of the 2008 5-day war. November 03, 2022. By Cameron Fraser.
30. Max-Planck-Institute: Surblyte, Gintare. (2011). The Refusal to Disclose Trade Secrets as an Abuse of Market Dominance – Microsoft and Beyond. (Münchener Schriften zum Europäischen und Internationalen Kartellrecht, 28), XLVII + 263 S., Stämpfli: Bern
31. E-spincorp.com: Reverse Engineering is legal or illegal? December 18, 2020.
32. Welt.de: Wenn der Kampf gegen „Desinformation“ dazu dient, Meinungen zu unterdrücken. (In German: If the fight against "disinformation" serves to suppress opinions). January 28, 2023. By Jakob Schirmmacher.
33. Transparency International EU: Vanishing Act: The Eurogroup's Accountability. February 05, 2019. By Vitor Teixeira.
34. Benjamin Zyla. (2020): The End of European Security Institutions? The EU's Common Foreign and Security Policy and NATO After Brexit. Springer: Berlin, p. 98 ff
35. FAZ.net: Wer Hass sät. May 13, 2017. By Michael Hanfeld. (In German: He who sows hatred.)
36. Welt.de: „Durchtränkt von Menschenfeindlichkeit“ – Böhmermann und Lanz liefern sich Schlagabtausch. September 07, 2021. (In German: „Soaked in misanthropy“ – Böhmermann and Lanz exchange blows)
37. Institut für Demoskopie Allensbach: Grenzen der Freiheit Eine Dokumentation des Beitrags von Prof. Dr. Renate Köcher in der Frankfurter Allgemeinen Zeitung Nr. 119 vom 23. Mai 2019 (In German: Limits of Freedom A documentation of the article by Prof. Dr. Renate Köcher in the Frankfurter Allgemeine Zeitung No. 119 of May 23, 2019.)

# PHOTO CREDITS | IMPRINT

## Photo credits:

Cover: graphic elements – kitka, abstract background – Olga each by stock.adobe.com  
P. 4 pickup by stock.adobe.com  
P. 12 commons.wikimedia.org/wiki/Egypt\_Abu\_Simbel  
P. 14 NATO Standard AJP-01(F), page 2  
P. 15 NATO Standard AJP-01(F), page 79  
P. 17 Christian Horz by stock.adobe.com  
P. 21 Montri by stock.adobe.com  
P. 22-23 maciek90 by stock.adobe.com  
P. 24 Fig 3: Coordination and logistics of cyber attacks. cybersecurityforme.com  
P. 27 Quelle: Stiftung Wissenschaft und Politik (SWP), ©Dr. rer. pol. Annegret Bendiek  
P. 28 Beyond Fake News. 10 Types of Misleading News. ©EAVI European Association for Viewers Interests. Source: <https://eavi.eu/beyond-fake-news-10-types-misleading-info/>  
P. 31 Hacking Statistics: Icons – LineSolution by stock.adobe.com and freepik.com  
P. 32 Grafics 10 biggest ransomware: cybersecurityforme.com. Illustration: Anch by stock.adobe.com  
P. 33 top left – xiaoliange, bottom left Artur, right – zochen each by stock.adobe.com  
P. 34 Ayesha by stock.adobe.com  
P. 36 [www.flickr.com/photos/itupictures/52753528559/in/album-72177720306795268/](https://www.flickr.com/photos/itupictures/52753528559/in/album-72177720306795268/)  
P. 37 [www.flickr.com/photos/itupictures/52752695332/in/album-72177720306795268/](https://www.flickr.com/photos/itupictures/52752695332/in/album-72177720306795268/)  
P. 40-41 Egor by stock.adobe.com  
P. 44-45 Denis Rozhnovsky by stock.adobe.com  
P. 46 Top 10 Emerging Cyber-Security Threats for 2030. ©ENISA European Union Agency for Cybersecurity. Published: November 11, 2022. Source : <https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030>  
P. 47 Fig 10: Conceptual diagram of security posture. ©2023 Balbix, Inc. All rights reserved. Source: <https://www.balbix.com/insights/what-is-cyber-security-posture/>  
P. 51 chungking by stock.adobe.com  
P. 52-53 collage – Energy: gopixa, hacker: ImageFlow each by stock.adobe.com  
P. 54 vchalup by stock.adobe.com  
P. 58 zatevakhin by stock.adobe.com  
P. 63 Rokas by stock.adobe.com  
P. 66 artsterdam by stock.adobe.com  
P. 68 victoria p. by stock.adobe.com  
P. 71 Fig 11: NATO STANDARD AJP-01(F), page 3; Graphic triangle – abert84 by stock.adobe.com  
P. 72 Who's Who in Russian Cyber Espionage? ©oodaloop.com. 2023 all rights reserved. Published: May 9, 2018. Source: <https://www.oodaloop.com/cyber/2018/05/09/whos-who-in-russian-cyber-espionage-operations/>  
P. 76 gankevstock by stock.adobe.com  
P. 78 Tada Images by stock.adobe.com  
P. 81 Melinda Nagy by stock.adobe.com  
P. 84 Firefly KI generiert  
P. 86-87 ©medium.com Source: <https://medium.com/magnetic/our-children-should-be-questioning-us-and-demanding-more-they-deserve-better-825e25a8197d>  
P. 88 Data: Enisa. Source: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021> and <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

P. 89 Global Cyber Strategies Index. Open Source: cybersecurityforme.com. Source: <https://cybersecurityforme.com/cybersecurity-infographics-facts-stats/>.  
Map – mapsandphotos, graphic Elements–Anch each by stock.adobe.com  
P. 99 NATO Standard AJP-01(F), page 49  
P. 104 CIA Triad. CC BY-SA 4.0 File: CIAJMK1209-en.svg Created: 5 February 2022 Creator: Michel Bakni. Source: [https://en.wikipedia.org/wiki/Information\\_security#/media/File:CIAJMK1209-en.svg](https://en.wikipedia.org/wiki/Information_security#/media/File:CIAJMK1209-en.svg)  
P. 110 gi0572 by stock.adobe.com  
P. 112 NATO STANDARD AJP-01(F), page 56  
P. 125 How to Spot Fake News. ©IFLA – International Federation of Library Associations and Institutions. Issue Date: Mar 2017. Source: <https://repository.ifla.org/handle/123456789/167>

## Imprint:

### ODISCYE Project Policy Compendium

Online Disinformation and Cyber Insecurities in International Politics

**Author:** Schubert, Lucas Maximilian M.A.  
Supervision: Stetter, Stephan, Prof. Dr.

First Edition: 25.11.2023

### Publisher:

© University of the Bundeswehr Munich  
Institute of Political Science  
Werner-Heisenberg-Weg 39  
85577 Neubiberg

### Design and Layout:

allegria design  
Jutta Oppermann  
Rotdornweg 35  
82024 Taufkirchen b. München  
[www.allegriadesign.de](http://www.allegriadesign.de)

### ISBN for PDF:

978-3-943207-76-7

### Printing:

Ecological printing with organic printing inks on picture printing paper, EU Ecolabel

### Climate-neutral production:

The CO<sub>2</sub> emissions caused by printing and production  
The CO<sub>2</sub> emissions caused by printing and production during the production of this brochure were neutralized  
The corresponding amount of CO<sub>2</sub> emissions will be offset.



Visit [www.natureoffice.com](http://www.natureoffice.com) for further details.

