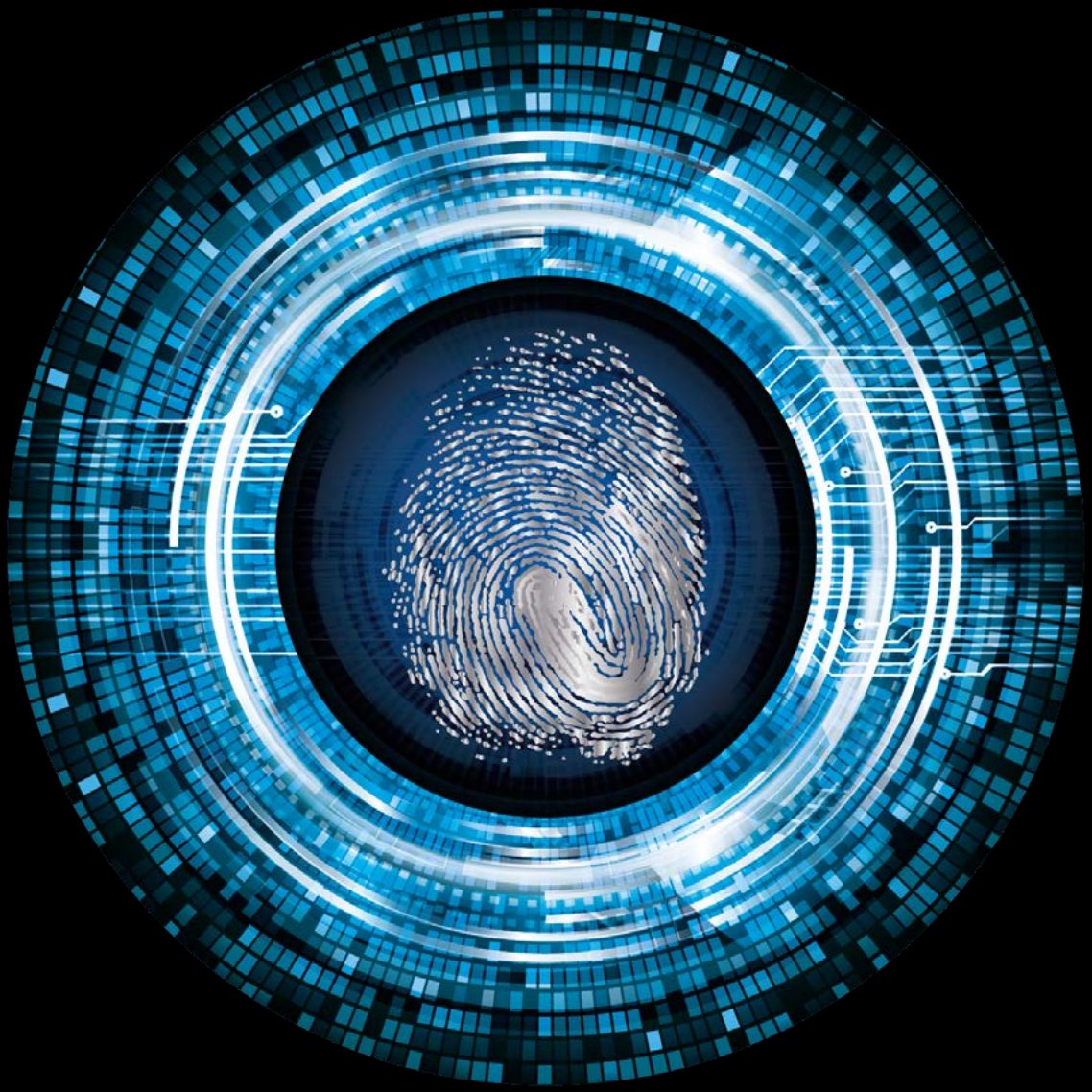
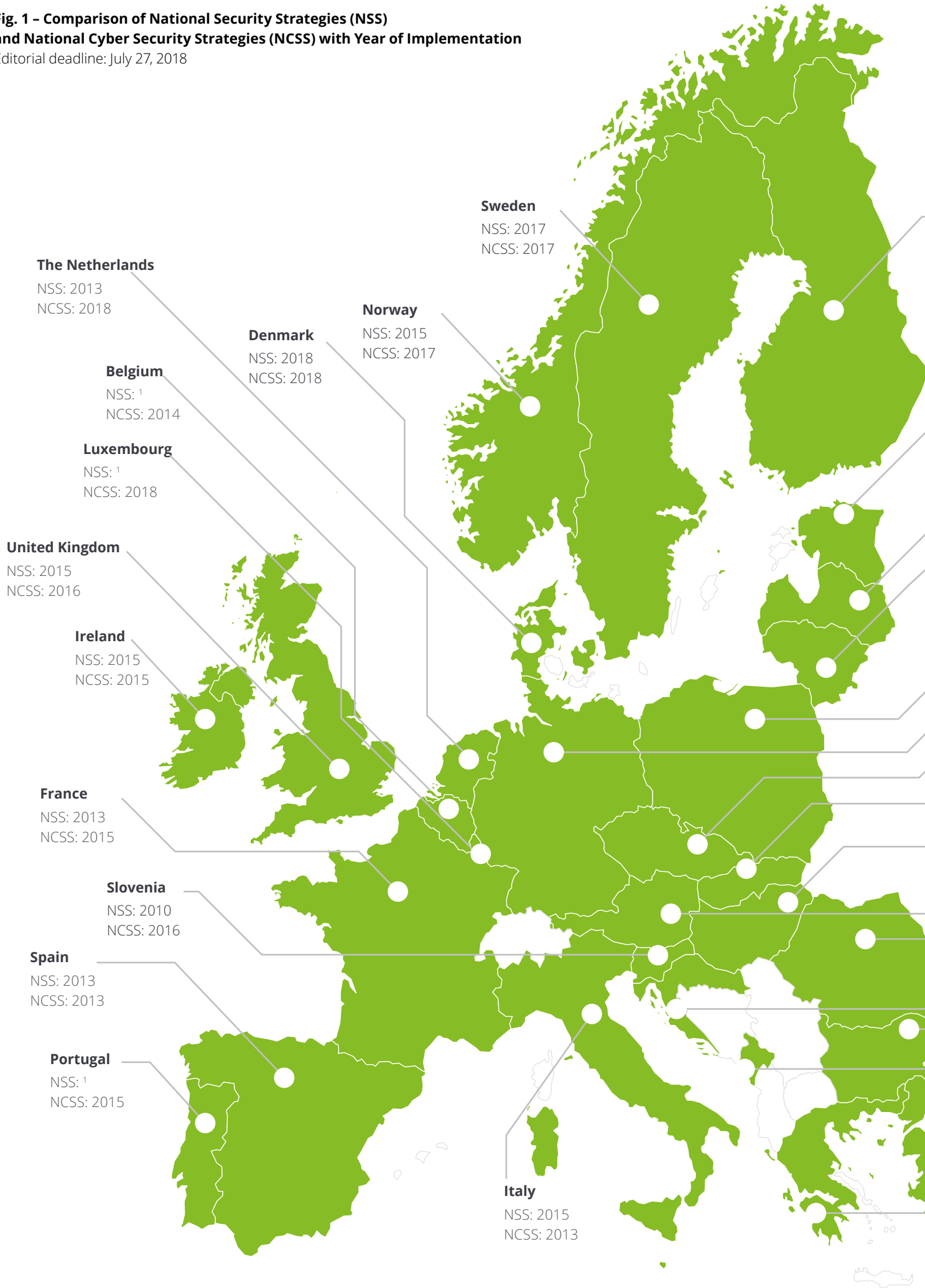
Deloitte.

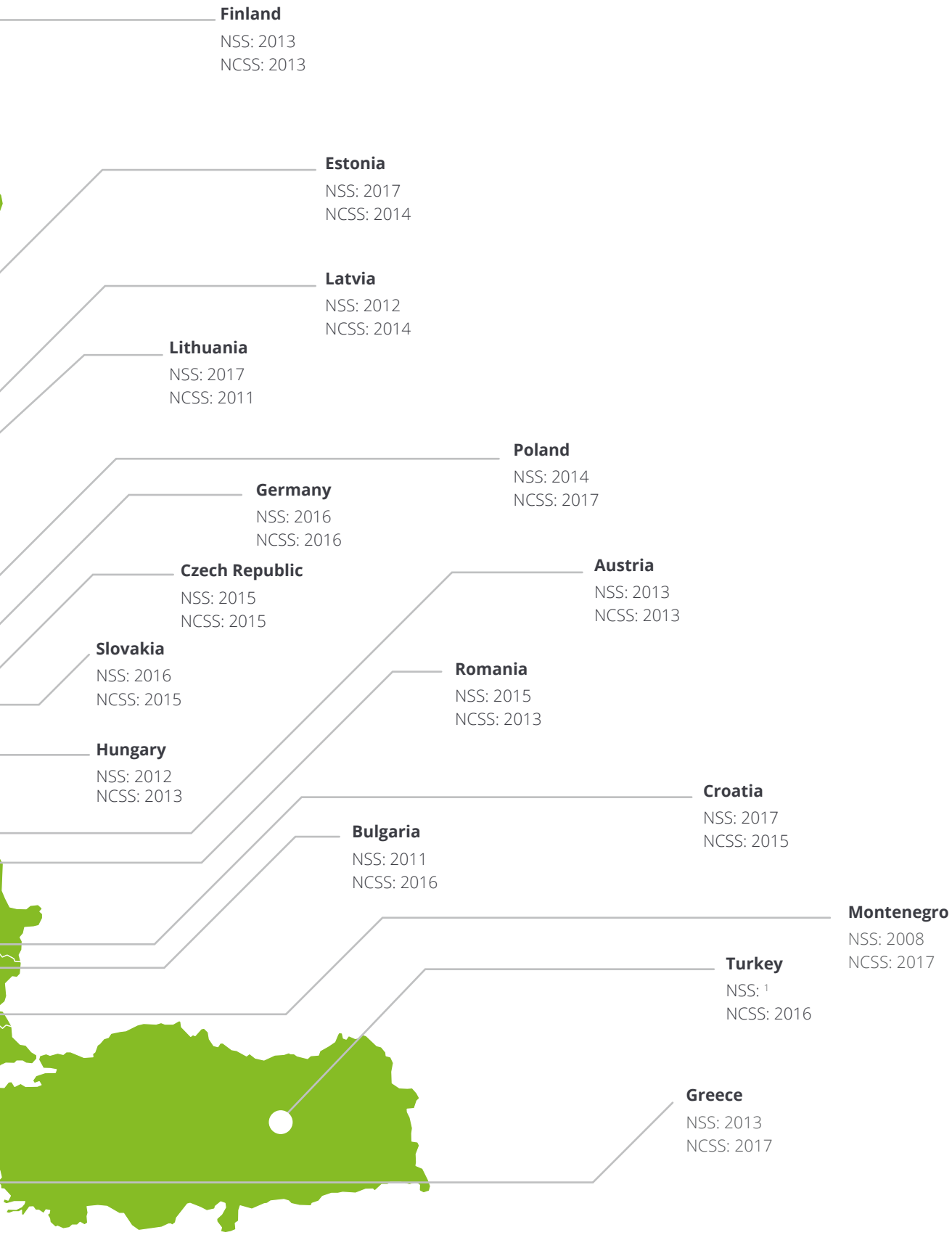


European Cyber Defense

Part 1: Strategies – Status quo 2018

Fig. 1 – Comparison of National Security Strategies (NSS) and National Cyber Security Strategies (NCSS) with Year of Implementation
Editorial deadline: July 27, 2018





Finland
NSS: 2013
NCSS: 2013

Estonia
NSS: 2017
NCSS: 2014

Latvia
NSS: 2012
NCSS: 2014

Lithuania
NSS: 2017
NCSS: 2011

Poland
NSS: 2014
NCSS: 2017

Germany
NSS: 2016
NCSS: 2016

Czech Republic
NSS: 2015
NCSS: 2015

Slovakia
NSS: 2016
NCSS: 2015

Hungary
NSS: 2012
NCSS: 2013

Austria
NSS: 2013
NCSS: 2013

Romania
NSS: 2015
NCSS: 2013

Croatia
NSS: 2017
NCSS: 2015

Bulgaria
NSS: 2011
NCSS: 2016

Montenegro
NSS: 2008
NCSS: 2017

Turkey
NSS: [1]
NCSS: 2016

Greece
NSS: 2013
NCSS: 2017

(without Malta and Cyprus)
[1] Not available in English.

Foreword

Cyber security is a government task. This is something countries in Europe agree about. But how can the state ensure cyber security in the interplay between business, science, and society? What are the threats to citizens and businesses in cyberspace? There are many different answers and approaches to these questions within Europe.

Our analysis of state structures and measures for cyber security has revealed that there is no current and compact overview of the European countries' various national strategies, protagonists, and initiatives. We hope to provide this overview in the first part of our report.

This report is the result of a systematic comparison of the relevant national strategy documents with statements about cyber defense. In this context, we understand cyber defense to mean all government activities designed to counter cyber risks. Another goal of this study is to analyze what the countries considered understand cyber defense to be.

We deliberately limited ourselves to the analysis of publicly available documents; these were essentially National Security Strategies (NSS) and, where available, National Cyber Security Strategies (NCSS). Our survey covers 29 countries that belong to the European Union and/or NATO; in some cases we have also included the cyber superpowers China, Russia, and the USA for comparison.

Differing perceptions of the challenge of cyber security lead to differing approaches to a solution; this is also reflected in the structure of the various strategy documents. In view of the strategic relevance, complexity, and dynamic nature of cyber security, it was important not to succumb to the proverbial danger of comparing apples and oranges. We therefore tried to identify categories that can be found in all strategies and compared the corresponding statements of the countries concerned. We oriented our analysis towards the following key questions:

„Guaranteeing freedom and security is one of the core tasks of the state. That also applies to cyberspace."

(Germany, Cyber Security Strategy for Germany 2016)

We are aware that there may be a discrepancy between the measures named in strategy documents and the extent to which such measures are implemented. However, in view of the objective of this report, we have neither assessed the statements in the individual strategy documents nor investigated the current status of the structures and measures.

The comparison of national strategies is supplemented by a summary of relevant documents, statements on objectives, and current initiatives by the European Union, NATO, and the United Nations.

Without wanting to anticipate the results of our investigation: the identified cyber risks, strategic goals, and the structures and measures derived from them in the various European countries differ, in some cases considerably. This status quo was not a great surprise in view of the relatively recent, yet dynamic challenge of cyber security.

However, all documents are based on a certain perception of the strategic context at the time of their preparation. In other words they are based on an individual assessment of the threat situation, the state's responsibilities and reach, and also the effectiveness of the technology and the measures taken by those preparing the documents at various times. The coordination of future strategies requires a great degree of common understanding of the possible development of key drivers that will determine the future strategic context.

This first part of the report is supplemented by a second part in which we have developed possible scenarios of cyber security in Europe in 2030.

With these two publications we hope to make a contribution to the much-needed debate between the state, the economy, and society, but also between individual state protagonists. Ideally our reports will help us all to find the right answers to the challenge of cyber security – or at least to ask the right questions.

Executive Summary

Technological progress, regulatory requirements and constant changes in the threat situation are key influencing factors in cyberspace. Developments are fast-paced and lead to serious challenges for states to ensure public safety and to coordinate international cooperation. These challenges must be taken into account in the development, implementation, and regular review of national (cyber) security strategies.

The present first part of the European Cyber Defense 2018 report is intended to provide an up-to-date and compact overview of the European countries' various national strategies, protagonists, and initiatives. The core of the report is a systematic comparison of European countries' relevant national strategy documents. Our systematic comparison has identified six possible fields of action. We are convinced that they will play a major role when national cyber security strategies are updated.

This first part of the European Cyber Defense report closes with 34 fact sheets on national and international cyber security strategies. The structure of the fact sheets is based on the guiding questions mentioned above. Each fact sheet shows concise key points of the individual strategies. For 32 states, the European Union and NATO, the objectives, cyber threats and the actors involved are summarized in a nutshell. The central and particularly relevant results are:

Most remarkable results are:

Almost half of the national security strategies and more than a third of the national cyber security strategies are four years old or older. Global cyber security incidents in the past four years don't really seem to have driven updates. In some cases, even self-defined fixed lifetimes of national cyber security strategies have been exceeded without an update being undertaken.

Cyber threats are considered one of the greatest national threats. Judging by the frequency with which it is mentioned in national security strategies, governments see the danger from cyber threats as predominant. They are mentioned in national security strategies alongside terrorism and organized crime. It is also noted that more and more conventional and unconventional methods are being used in combination (hybrid warfare) or that state and non-state actors are acting together. Attacks often take place below the threshold of armed conflict. In the totality of all cyber security strategies considered, data and identity theft as well as espionage are described as the most common threats. Both threats are global cyber crime phenomena and may also be part of hybrid threats.

Data and identity theft as well as espionage are described as the most common threats in the sum of all considered cyber security strategies. Both threats are global phenomena of cyber crime.

In some cyber security strategies, it is difficult to recognize a clear division of responsibilities at state level. Responsibility is frequently distributed over several departments and hierarchy levels. The great importance attached to hybrid threats also calls for a networked approach. However, this cannot always be recognized in the structures described.

The use of uniform definitions of certain concepts of cyber security is not entirely given. Although NATO maintains a glossary of definitions, many governments define individual terms themselves or in some cases interpret them differently.

1. National perspective: strategic risks and the importance of cyber security

What risks are mentioned in the security strategy and what is the significance of cyber security?

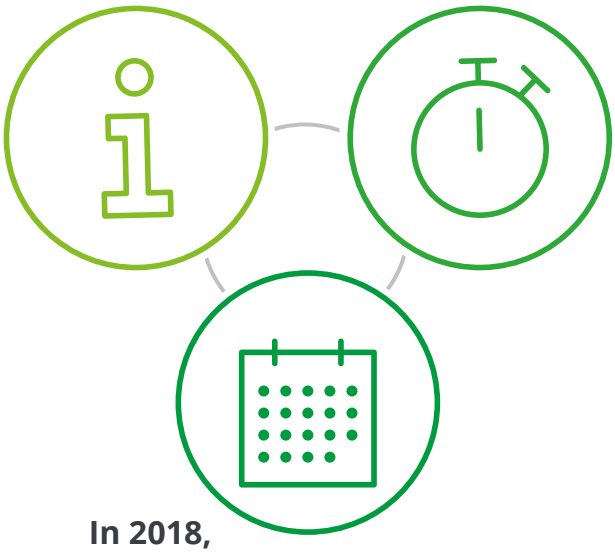
National security strategies are the supreme fundamental security policy documents of governments. They make a strategic assessment of the current position and name the interests, priorities, and objectives of national security policy. The strategies are usually forward-looking in order to anticipate crises and conflicts and to react appropriately to dangers. Often they are also security policy reports and declarations of action by governments to their national parliaments. As the supreme security policy documents, they are also the basis of a national cyber security strategy. Accordingly, the starting point for comparing national cyber security strategies should be a comparison of national security strategies (NSS).

A long-term but also current strategic assessment of position is becoming increasingly difficult for European governments. The security situation is becoming more complex, dangers are less predictable than in the past. Security strategies must take this complexity and the resulting uncertainty into account. In this section we show which threats have been identified in national security strategies and how they are classified with reference to cyber threats, if cyber threats have even been recognized as national threats. In addition, the age structure of the strategies is analyzed.

Twenty-five national security strategies are publicly available. Half of them are four years old or older.

Fig. 2 – Noticeable facts about national security strategies [2]

Almost half
of the national security strategies are four years old or older.



10 years ago,
the oldest national security strategy, that of Montenegro, was put into effect.

In 2018,
the most recent national security strategy, Denmark, came into force.

Denmark's national security strategy came into force in 2018. Denmark thus has the most up-to-date security strategy of the countries in the focus of this study. By contrast, Bulgaria, Estonia, Hungary, Latvia, Montenegro and Slovenia have strategies which came into force in 2012 or in some cases even go back to 2008. In the years since, many crises and conflicts have changed the global security situation. For example, the global financial crisis in 2007, the Caucasus conflict in 2008, the worldwide transmission of an H1N1 influenza pandemic in 2009, the Arab Spring (and the related conflicts in Iraq and Syria) in 2011, the euro crisis in 2012, the NSA affair in 2013, the Ukraine conflict in 2014, the refugee crisis in 2015 and above all countless terrorist attacks, including in Brussels, Nice, Paris and Berlin affected world affairs. But these events are not explicitly mentioned in the individual strategies – simply because in some cases the publication date of the strategy preceded the events. Nevertheless, the question arises – especially with regard to the relatively new phenomenon of cyber threats – whether future strategies are updated in shorter cycles in order to take into account the findings of such attacks, or whether strategies deliberately remain generic without explicitly referring to individual events.

China's and Russia's national security strategies came into force in 2015 and that of the USA in 2017. This means that the strategies of major global players are more recent than the average age of the European security strategies compared here.

The possibilities of cyberspace are constantly generating new challenges, threats, and risks. Frontiers are melting away, and regional, indeed even local events can have global effects. The dividing line between external and internal security has been largely dissolved in cyberspace.

[2] Excluding NSS of Belgium, Luxembourg, Portugal, Turkey.

Cyber attacks are comparatively inexpensive, easy to perform and it is difficult for defenders to attribute the origin of an attack unequivocally. The sources and intentions of an attack are of a manifold nature. They can originate from the military, the secret services, extremists, terrorists, organised crime or even from individual perpetrators.

„As access to software with great damage potential is comparatively easy and cheap, thanks also to proliferation, the means necessary for cyber attacks are not limited to states. Terrorist groups, criminal organizations, and well-versed individuals can also potentially do considerable damage with little effort. This means that efforts to create internationally binding regulations or confidence- and security-building measures are confined within narrow limits“

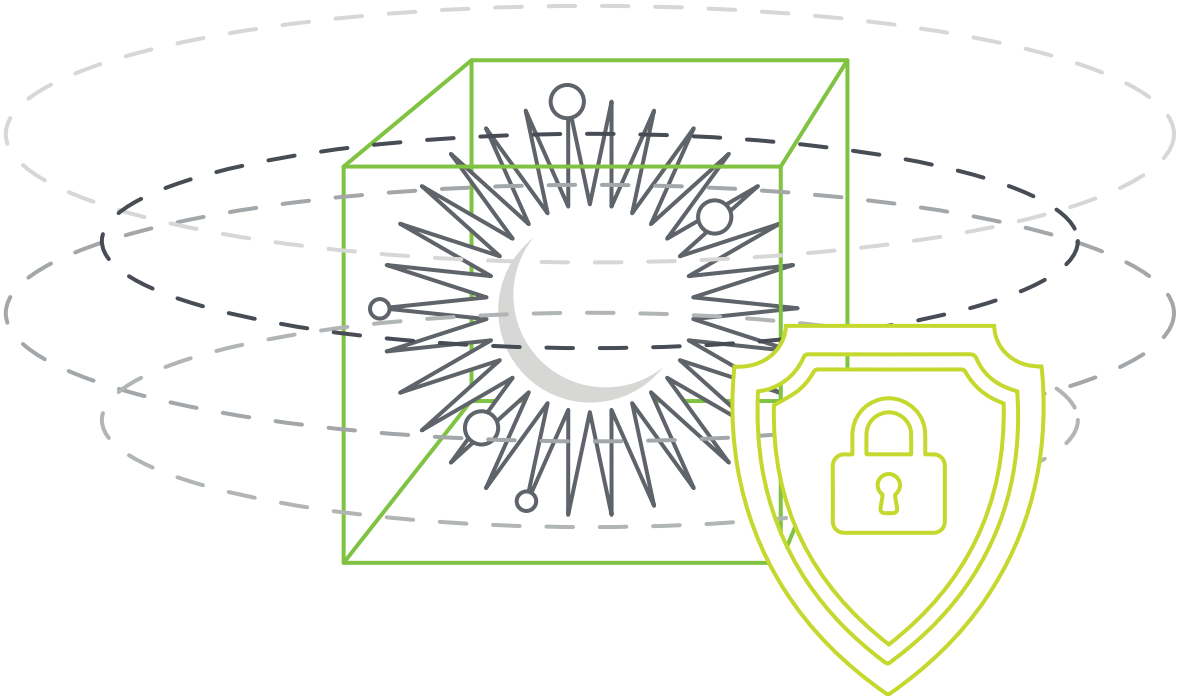
(Germany, White Paper on German Security Policy and the Future of the Bundeswehr 2016[3])

State safety precautions must be viewed holistically. They must include the entirety of measures aimed at protecting nations and maintaining the basis of existence of societies. Measures to protect cyberspace are indubitably part of this.

„Like terrorism, this is not simply a risk for the future. Government, the private sector and citizens are under sustained cyber attack today, from both hostile states and criminals. They are stealing our intellectual property, sensitive commercial and government information, and even our identities in order to defraud individuals, organisations and the Government.”

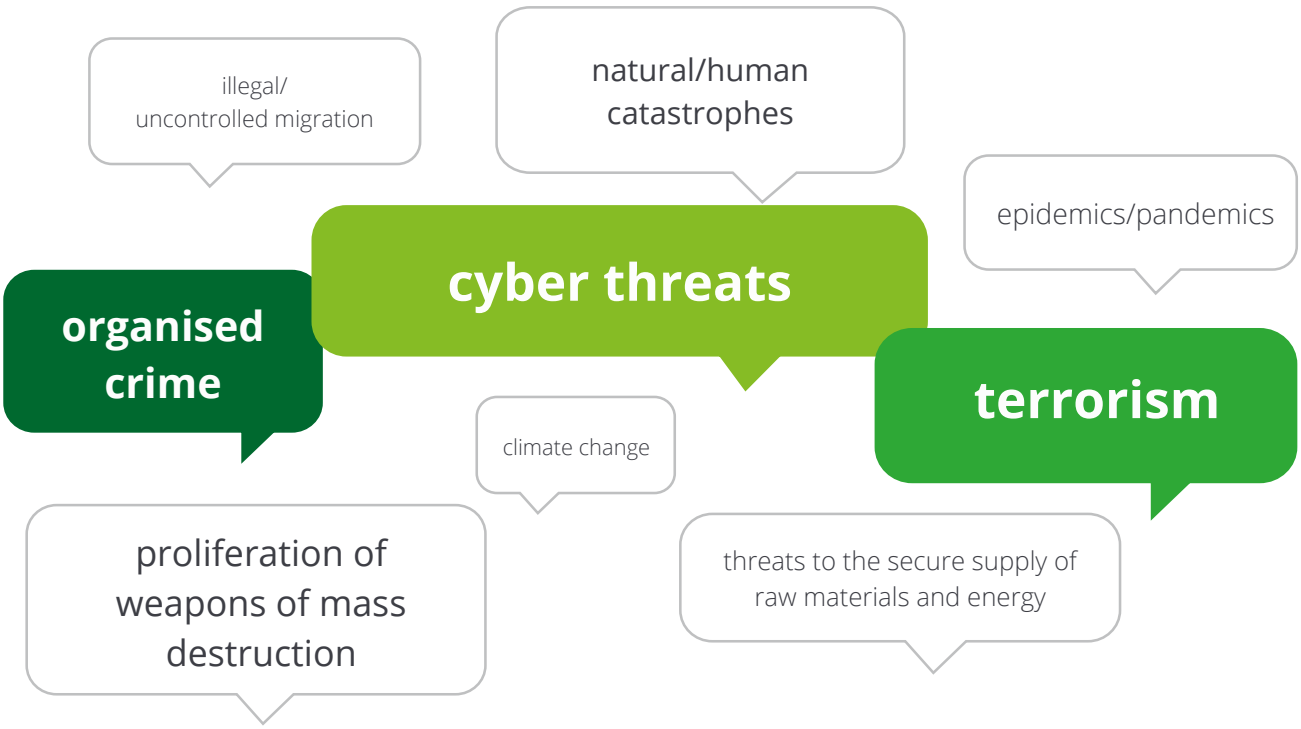
(United Kingdom, Prime Minister, National Security Strategy 2010)

[3] From henceforth „White Paper 2016“



Our analysis shows that governments have recognized the national threat from and within cyberspace. Cyber threats are most often cited as a national threat, along with terrorism and followed by organized crime. All security strategies discussed address cyber threats. However, national strategies are not based on a uniform definition of cyber threats. The term is used differently in the individual strategies and as a synonym for e.g. cyber threats, cyber attacks or cyber terrorism.

Fig. 3 – National threats and mapping of cyber threats to national security strategies[4]



[4] According to the number of mentions in the strategies considered.

In its current security strategy, the French government places cyber attacks on a par with terrorism, nuclear armament, and pandemics.[5] At the same time, it emphasizes that these threats have become even more urgent and that they must be countered by international cooperation.

The United Kingdom stands out with its classification of national dangers. Thus, for example, it carried out a comprehensive risk assessment in 2015, for the third time following 2010 and 2012. In these, national and international risks were derived and the probability of their occurrence and their scope were assessed. On this basis, the risks with the highest priority were defined. Cyber threats were assigned the highest priority, along with five other national threats.[6]

In its 2016 White Paper, Germany provides its current basis for the country's national security policy. The Federal Government writes that networking and the dissemination of risk are driven by globalization. Apart from information operations, epidemics, and terrorism, the possibility of cyber attacks is specially addressed. It should be emphasized that the Federal Government occasionally includes definitions in the White Paper, e.g., cyberspace and information space.

„In our globalised world, the safe, secure and free use of the cyber and information domain is a fundamental prerequisite for the activities of both the state and private individuals. Increasing digitalisation in all walks of life and the increasing interconnectivity of individuals, organisations and states are playing a unique role in our present and future opportunities. This development has, however, made the state, society and the economy particularly vulnerable to cyber attacks. As a consequence, urgent steps are needed to protect against threats."

(Germany, White Paper 2016)

[5] French White Paper (2013), p. 7.
[6] National Security Strategy and Strategic Defence and Security Review 2015.

The digital interconnectedness of people, companies, and states in Europe is accelerating more and more. Infrastructure such as energy supply networks, payment systems, communication networks and others, are crossing national frontiers. In cyberspace, national borders are also losing importance as safety barriers. The distinction between internal and external security is becoming more difficult to make and a community's uniform standards in cyberspace are becoming increasingly important, especially on security issues. In cyberspace too, a community is only as strong as its weakest link. An outdated national security strategy could be such a weak link. For example, it might not cover altered threat situations or not take the current state of the art into account.

Montenegro has by far the oldest security strategy; it came into force in 2008. Threats from cyberspace are mentioned here as a national risk, but no prioritization over other risks can be recognized. Montenegro is part of a region that was exposed to dynamic changes in recent years. The government sees the security situation in a regional context. In strategy matters, Montenegro generally refers to NATO's strategic approach and shares its evaluation of risks and threats to national security without explicitly addressing them. The government briefly mentions the increasing use of information technology. It sees a threat from cyber crime, especially to the transport infrastructure, telecommunications, health and social systems, the financial system and provisioning the population. Montenegro does not prioritize cyber threats over other national threats.

Governments expect terrorists and organized crime structures to use cyber attacks as a tool to support their operations. Some countries expect cyber attacks increasingly to become part of what is referred to as "hybrid warfare" or "hybrid attacks". These attacks combine conventional and non-conventional military operations with civilian means, or cyberspace is used as a tool for information warfare and propaganda. The objective is to obscure distinctions (e.g., between war and peace or between ally and enemy) in order to confuse the potential opponent and limit their opportunities to respond.[7]

[7] According to Schmid, Johann: Hybride Kriegführung und das "Center of Gravity" der Entscheidung (Hybrid Warfare and the Center of Gravity of the Decision), in: Sicherheit und Frieden (Security and Peace) 2/2016, pp. 114-120.

Nearly all governments describe a networked security approach in their national security strategies as a response to the underlying security situation and in particular as a response to hybrid threats. A networked approach is intended to improve the coordination of a wide range of protagonists. It should use military and civilian means to ensure sustainable stability, security, and peace. In the national security strategies compared here, responsibility for security precautions is attributed to a wide range of protagonists in the state, business, and society.

As for cyber-attacks: „It could therefore constitute a genuine act of war."

(France, White Paper 2013)

Military forces are assigned a central role in responding to attacks against the population concerned. The majority of the countries state that they are training military units for defense and operations in cyberspace.

„Cyberspace has become a new operational domain of conducting combat activity."

(Slovakia, White Paper 2016)

A comparison of national security strategies shows that cyberspace cannot be perfectly defined and differentiated from other areas of operation. We believe that uniform definitions and threat assessments will have a high priority in future. Almost no national security strategy defines these terms. The Spanish government defines cyberspace in its national security strategy:

„Cyberspace, a new area of relations which has spurred the development of new information and communication technologies, has blurred borders, making possible an unprecedented globalisation that provides new opportunities but entails serious risks and threats."

(Spain, The National Security Strategy 2013)

While the Spanish government's definition is rather abstract, the German definition is more detailed and distinguishes the terms cyberspace and information space. It makes a spatial distinction between information technology systems and information processing systems. These two different interpretations of the term cyberspace alone show that the national strategies are not currently based on a uniform definition.

„The information space is the space in which information is generated, processed, distributed, discussed, and stored. Cyberspace is the virtual space of all information technology systems that are networked or can be networked worldwide at the data level. Cyberspace, as a publicly accessible network of connections, is based on the internet, which can be extended by a random number of other data networks"

(Germany, White Paper 2016)

In its national strategy, the Lithuanian government defines cyber threats and highlights the state, critical infrastructures, and the citizen as goods to be protected.

„Cyber threats – actions in the cyber space aimed at disturbing the functioning of critical information infrastructures, activities of state institutions and economic sectors of importance for national security, obtaining classified or any other non-public information, committing other criminal acts and thus impairing the security of the State and its citizens."

(Lithuania, National Security Strategy 2017)

When governments define cyber security terms, they usually do so within the framework of national cyber security strategies. Some of these terms are presented in the following section.

According to the World Economic Forum, China, Russia and the United States are among the superpowers with the most advanced cyber capabilities.[8] But they do not provide a clear definition of cyberspace or cyber threats in their national security strategies. It is nevertheless worth taking a look at their national security strategies to compare their classification of cyber threats in relation to other national threats. China implemented its national security strategy in 2015.[9] No prioritization of cyber threats as against other national threats is undertaken. However, the government clearly points out that strategic competition in cyberspace has reached new dimensions and that this kind of warfare is accelerating. The Chinese Ministry of National Defense notes that the world's major powers are adapting their national security strategies to this acceleration as well as restructuring their military.

The Russian Federation also renewed its national security strategy in 2015. The government does not provide any indication of a clear prioritization of national threats. However, it emphasizes that all activities related to the use of information and communications technologies to spread and promote ideologies such as fascism, extremism, terrorism, and separatism, are a major threat to state and public security. The Russian government thus sees the spread of ideologies in cyberspace as a greater danger than the dangers that can attack or destroy vital IT infrastructures.

In contrast to the Russian Federation, the United States carries out risk identification emphasizing the security and resilience of its critical infrastructures and not primarily with regard to the diffusion of ideologies. They prioritize risks and their protection efforts, capabilities, and defenses according to the catastrophic or cascading consequences of cyber attacks. The USA's national security strategy came into force in 2017.

[8] "The countries which are believed to have the most developed cyber warfare capabilities are the United States, China, Russia, Israel and the United Kingdom"; https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/

[9] Chinese Military Strategy (2015): White Paper.

2. Objectives and assertions of national cyber security strategies

Which goals, responsibilities and risks are addressed in the cyber security strategy?

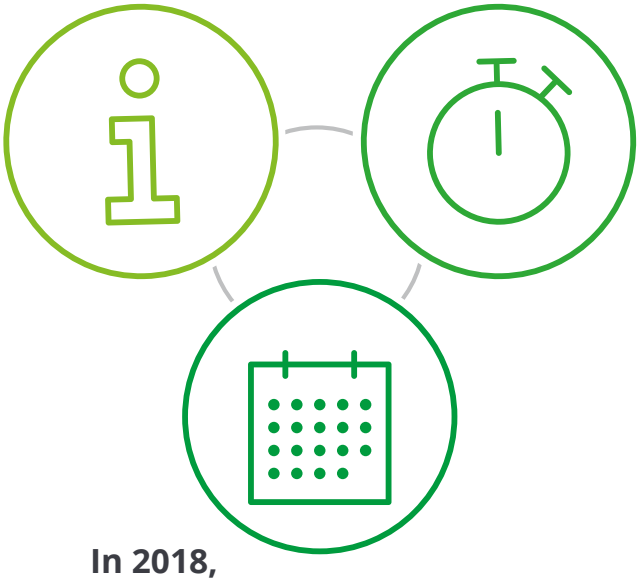
Cross-border cyberspace opens up opportunities and holds risks. It demands new approaches and new fields for government action. The state has a duty to meet constant changes and to create framework conditions in the interest of its citizens. With a national cyber security strategy, a government can put a fundamental document on cyber security into effect and set the course for a nation's future cyber security policy. The government can define strategic guidelines, demarcate areas for action, define cross-departmental responsibility and appoint protagonists.

This section contains a condensed comparison of 29 national cyber security strategies and shows, in essence, which targets are described in the strategies and which cyber threats are named by the governments. The first step is to compare when the national cyber security strategies came into force.

More than a third of current national cyber security strategies are four years or older. Denmark and Luxembourg have the most recent cyber security strategies, which were implemented in 2018. Lithuania has the oldest cyber security strategy, which was introduced in 2011. Since then, seven years have passed. Despite numerous cyber attacks in recent years, such as the malware Stuxnet from 2010 and Shamoon from 2012, as well as the ransomware Wanna Cry and the wiper malware Petya from 2016, older strategies have not been adapted.

Fig. 4 – Overview of national cyber security strategies

More than a third
of national cyber security strategies are four years or older.



7 years ago
the oldest national cyber security strategy, that of Lithuania, was put into effect.

In 2018,
the latest cyber security strategies were implemented by Denmark and Luxembourg.

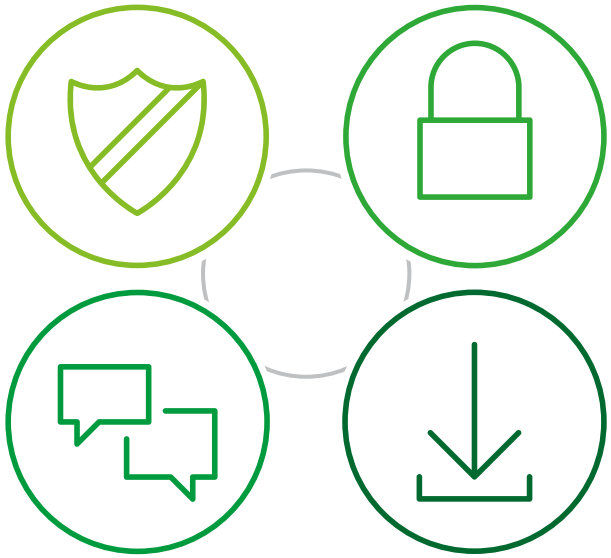
Governments could achieve recurrent consideration of or updates to a strategy through fixed lifetimes. Reaching the end of the lifetime certainly does not invalidate the national cyber security strategy, but the likelihood of an update in good time increases with the approach of the end of the lifetime. A fixed lifetime can be a binding guideline for recurrent consideration. In the documents before us, only eleven out of twenty-eight governments have added a fixed lifetime to their cyber security strategies. Estonia and Ireland are two of the countries that have added a fixed lifetime to their cyber security strategy, but they have already exceeded their self-imposed lifetimes without updating.

The national cyber security strategies or comparable documents with cyber security principles from China[10], Russia[11] and the USA[12] are on average more up-to-date than the European documents. Russia enacted its Cyber Security Strategy in 2014, the USA its Cyber Strategy in 2015, and China its Cyber Security Law in 2016.

With a clear definition of objectives, governments can enable a forward-looking cyber security policy and fully exploit the opportunities of cyberspace for the benefit of their societies. With them they can also make risks in cyberspace controllable. Objectives are defined in all the strategies examined. In 2 out of 29 cyber security strategies, safeguarding crucial infrastructure is set as an objective. Only the Norwegian government does not directly mention this objective. Indirectly, however, they describe a pilot project aimed at creating a functioning market for companies and users of crucial infrastructure.

[10] Cyber Security Law of the People's Republic of China (2016)
[11] Russian Cyber Security Strategy (2014)
[12] The DoD Cyber Strategy (2015)

Fig. 5 – Striking key objectives of national cyber security strategies[13]



97%
see critical infrastructure security as a goal

93%
have set the goal of secure and robust information systems

7%
rely on a fast response to cyber attacks

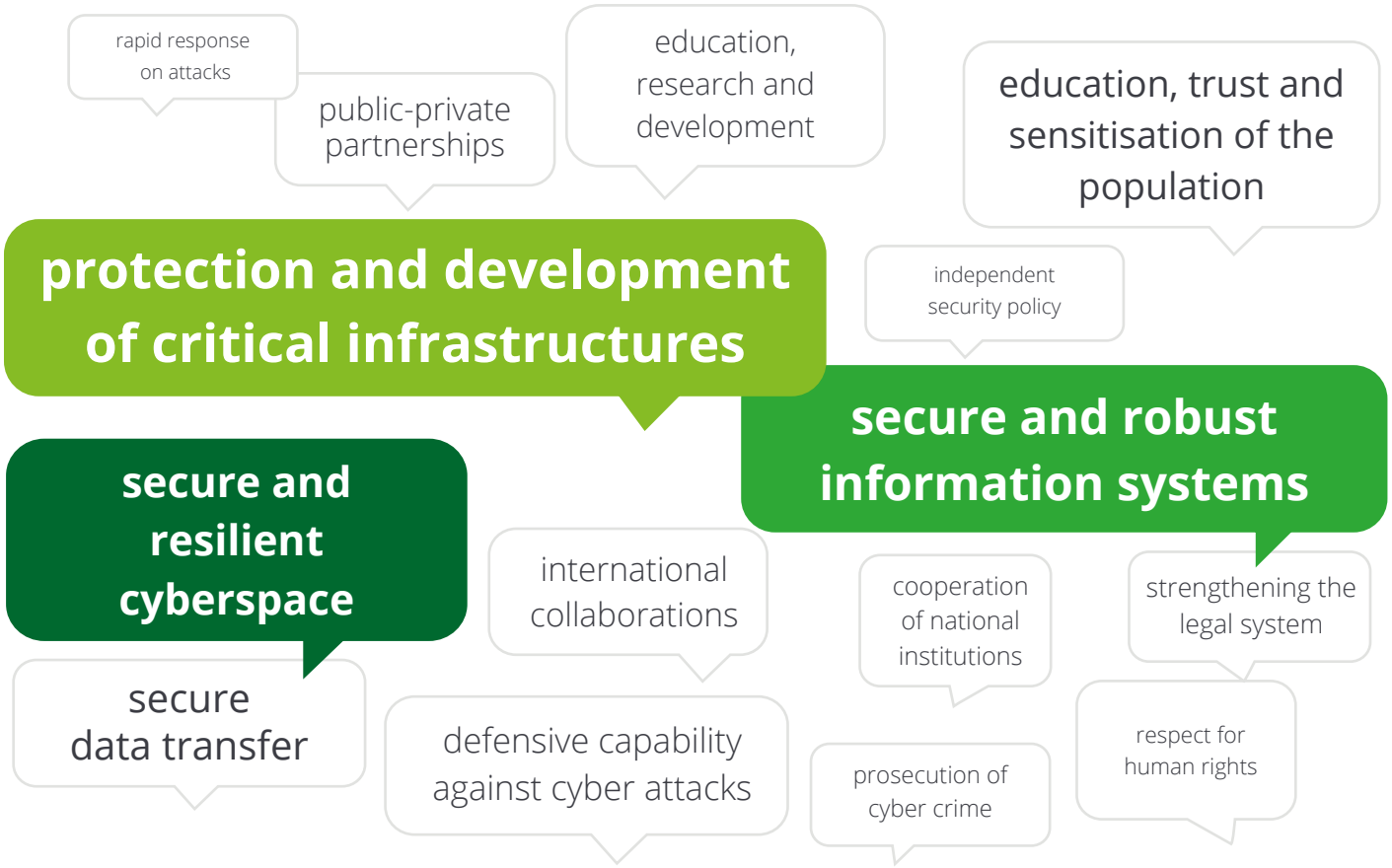
76%
define secure data transfer as their goal

Secure and robust information systems are the second most frequently mentioned goal. France, for example, mentions this objective in a prominent position and as a political response to the cyber attacks that are taking place round the world. In its White Paper, the French government states that robust information systems must go hand in hand with coordinated organization and operational cooperation between various government agencies in order to withstand cyber attacks. Montenegro and Portugal are the only two countries that do not mention this objective directly, or at least not literally. They place greater emphasis on secure data transfer, which is also mentioned by almost three quarters of the national strategies examined.

Only 2 out of 29 governments, UK and Slovenia, mention rapid responses to cyber attacks in their current strategies. The UK is not only planning a hub of social and economic experts with its National Cyber Security Centre (NCSC), but the government is also planning it as an organization from which to respond quickly to major threats. Slovenia has defined measures in its cyber security strategy to make it easier for its national cyber security system to respond quickly. Reactions to cyber attacks are mentioned in nearly all other cyber security strategies, but no time line is established. The term "rapid" is also not defined in detail in the United Kingdom or Slovenia. It remains unclear in both strategies whether this means proactive or only reactive rapid measures.

[13] As a percentage of the responses in the strategies considered.

Fig. 6 – Core objectives of national cyber security strategies[14]



[14] According to the number of mentions in the strategies considered.

Compared to the national security strategies, the national cyber security strategies contain adequate definitions of terms on a larger scale, in some cases adding glossaries. The Austrian government has one of the most comprehensive glossaries. In its "Cyber Security Glossary" it defines 29 terms in connection with cyber security. They define cyber security as follows:

„Cyber security describes the protection of a central legal interest by constitutional means against actor-related, technical, organizational, and natural hazards that endanger the security of cyberspace (including infrastructure and data security) and the safety of cyberspace users. Cyber security helps to identify, assess, and track threats and to strengthen the ability to manage disruptions in and emanating from cyberspace, mitigate the associated consequences and restore the ability of the protagonists, infrastructure and services concerned affected thereby to act and function."

(Austrian Strategy for Cyber Security 2013)

The Austrian definition of cyber security is comparatively more detailed than others. It understands cyber security to mean not merely the security of infrastructure, data and related services, but also explicitly the security of users. Denmark and Turkey are less comprehensive in their definitions, as they only consider data, systems, and related services.

„Cyber security provided at a national scale for any hardware and software systems associated with all services, transactions, information/data provided through the information and communication technologies that constitute national cyber space."

(Turkey, National Cyber Security Strategy 2016 to 2019)

„Cyber security encompasses protection against breaches of security resulting from attacks on data or systems via a connection to an external network or system. Cyber security thus focuses on vulnerabilities inherent to the interconnection of systems, including connections to the Internet."

(Denmark, Danish Cyber and Information Security Strategy 2018)

„Cyber security is the IT security of information technology systems that are networked or can be networked at the data level in cyberspace."

(Germany, Cyber Security Strategy for Germany 2016)

The German Federal Government's definition is one of the narrowest and defines the term cyber security, in a similar manner to Turkey and Denmark, with regard to the data level and at the level of information technology systems.

Regardless of the definitions, all reviewed countries recognize threats in cyberspace. They recognize that cyber attacks on states and critical infrastructures have long been a reality and that attackers do not shrink from developed countries and digitalized armed forces, but rather see them as a worthwhile target. More than half of the national cyber security strategies under review cite data and identity theft along with espionage as cyber threats. Both threats are global cyber crime phenomena. These are crimes that are committed using information and communications technology or are directed against them.[15] The prosecution and combating of cyber crime at the national level is handled differently in the countries under consideration, as a rule by organizations with policing tasks. At the international level, no country can solve these phenomena by itself and cooperation is becoming increasingly important. The European Cyber Crime Centre (EC3) at Europol and Interpol combat cyber crime at the international level.

Fig. 7 – Most frequently identified threats according to national cyber security strategies[16]

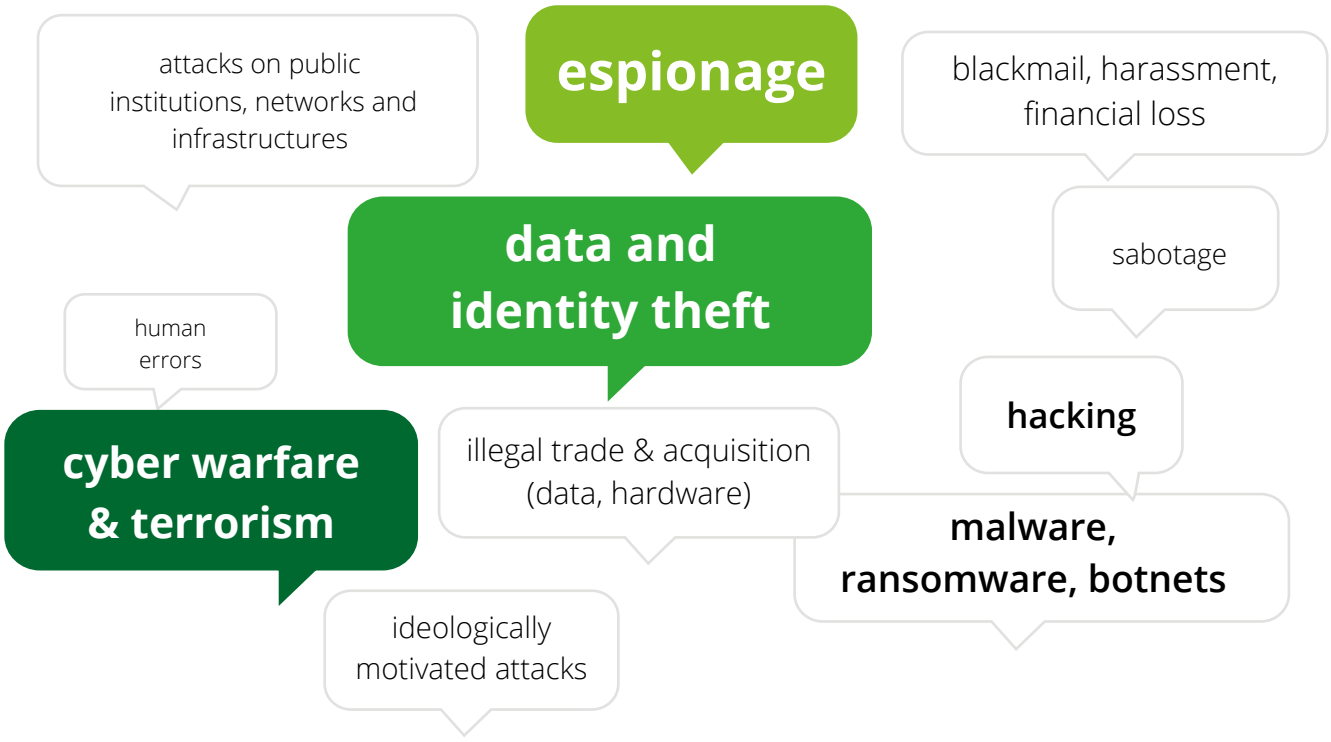
More than half
of the national cyber security strategies examined cite data and identity theft as a threat.

[15] BMI (2018), http://www.bmi.bund.de
[16] As a percentage of the responses in the strategies considered; USA, China and Russia cite these cyber threats in their national cyber security strategies.

China and the USA also see these cyber crime phenomena as major threats to national cyber security and identify them explicitly in their national cyber security strategies. Russia does not name these phenomena. In the Russian cyber security strategy, threats in cyberspace are considered dependent on the ability to disseminate information. Russia sees the danger that information and communications technologies will be used as weapons to disseminate information. They see the threat in the disruption of public order and the spread of hatred and terrorism.

Cyber terrorism, malware, ransomware, botnets and hacking are further threats most frequently mentioned in the national cyber security strategies in the comparison. Human errors, disloyal employees or social engineering are seen as cyber threats much less frequently in the strategies, although the human risk factor is seen as the greatest danger for companies in the current Cyber Security Report by the Allensbach Institute and Deloitte.[17]

Fig. 8 – Threats according to national strategies[18]



[17] Deloitte, Cyber Security Report 2017, Part 2, p. 14.
[18] According to the number of mentions in the strategies considered.

These and many other threats in cyberspace affect the objectives of cyber security – confidentiality, integrity, and availability. Cyber attacks even use information technology to target one or more IT systems and the objectives of cyber security directly and intentionally. Effective protective steps can be taken to reduce the security risk to an acceptable level. Cyber security is a nation-wide task and is increasingly ensured by cooperation across political department boundaries. In addition to territorial integrity and sovereignty, the security of a state also must be defended in cyberspace. Cyber Defense, as a term, is interpreted differently in the national cyber security strategies under consideration. In Germany and Austria, Cyber Defense tends to group together the military means of defense that are especially suited to this purpose.

„Cyber Defense comprises the defensive and offensive capabilities available within the Bundeswehr (Federal Armed Forces) in the framework of its constitutional mandate and international law to operate in cyberspace, which are suitable and necessary for mission and operations management or for defending against (military) cyber attacks and thus for protecting its own information, IT, and also weapons and weapons systems. This also includes the use and co-design of structures, processes, and reporting systems of cyber defense under defense-related aspects and situations"

(Germany, Cyber Security Strategy for Germany 2016)

The term Cyber Defense is interpreted in a more general and less military manner in the international context. It frequently includes all tasks that protect and restore IT systems and detect and respond to threats.

„The application of effective protective measures to obtain an appropriate level of Cyber Security in order to guarantee Defence's operation and functionalities. This is achieved by applying appropriate protective measures to reduce the security risk to an acceptable level. Cyber Defence consists of following duties: Protect, Detect, Respond, and Recover."

(Belgien, Cyber Security Strategy for Defence 2014)

The Swedish government goes one step further and states that active operations are also part of Cyber Defense.

„Cyber defense capabilities are an important part of the [...] Defense. Vital systems must be protected from attack. This also requires the ability to carry out active operations in the cyber domain."

(Sweden, Sweden's Defense Policy 2016 to 2020)

The national cyber security strategies in Germany, Finland, France, the UK, the Netherlands and Slovakia likewise mention offensive measures and capabilities to protect their own systems and information in cyberspace. In their strategies, Belgium and Portugal provide a view of the development of future offensive capabilities. NATO defines proactive measures to detect possible cyber attacks or to determine the origin of a cyber operation, using the term Active Cyber Defense. This can also be preventive cyber operations against the source of a possible cyber attack.[18]

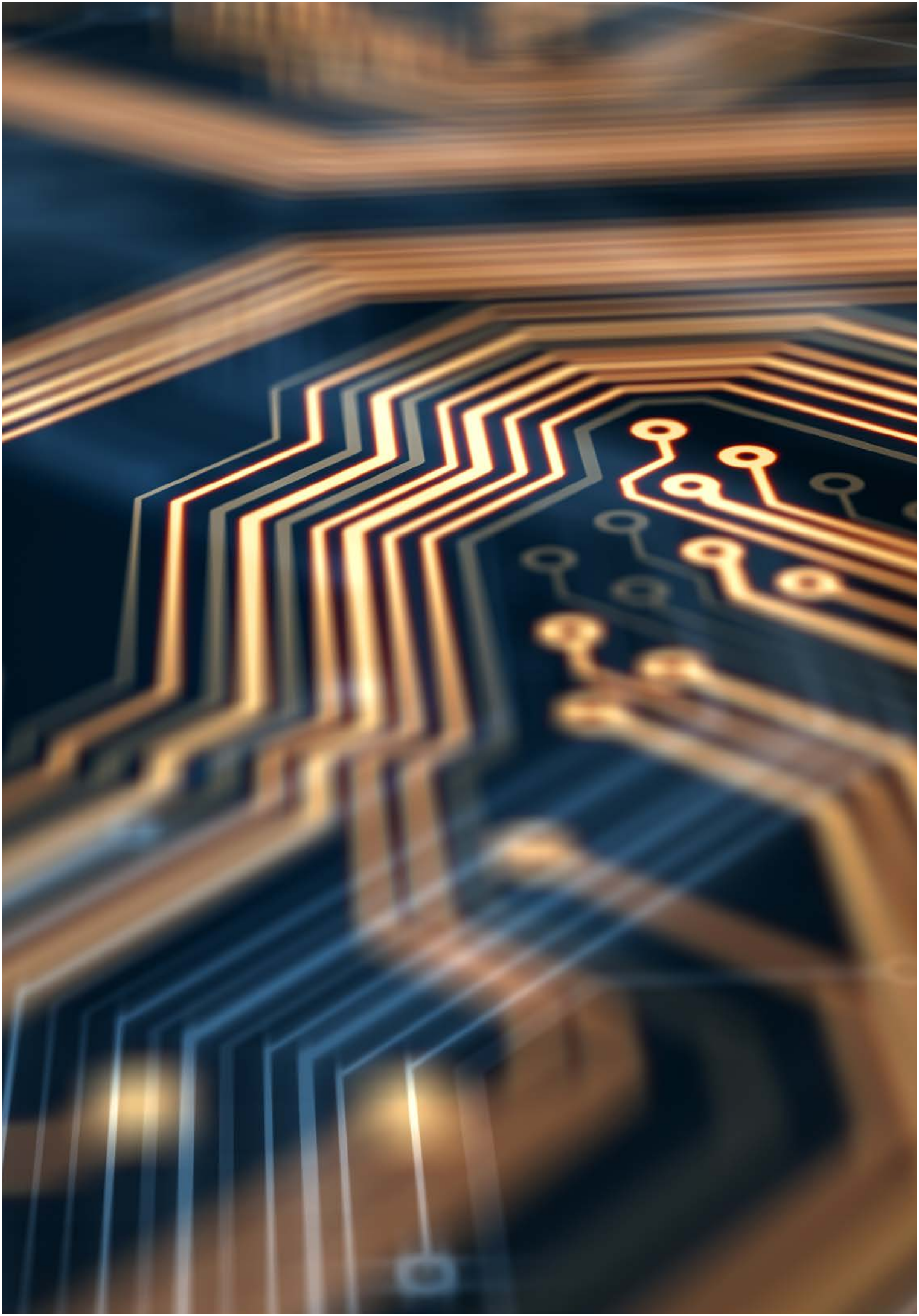
„The more competent and careful the opponent, the more difficult the attribution. But even the best hackers make mistakes, so there is often a chain of indicators that point to a certain group. The more qualified the opponent, the harder it is to counterattack, especially when shooting from the hip. Complex cyber attacks require a great degree of knowledge of the target system and its deployment context."

(SWP-Aktuell, Journal of the German Institute for International and Security Affairs no. 59, August 2017)

Active Cyber Defense and preventive cyber operations are a topic of controversial discussion. Examples are whether conventional means may also be used actively to respond to a cyber attack and how to deal with a possible false attribution of the opponent.

The distinction between active and defensive measures in cyberspace cannot be clearly delineated. Active defense should be tailored to the potential attacker in order to be effective. For this purpose the defender should obtain knowledge of system-specific vulnerabilities. We are of the opinion that Active Cyber Defense will strengthen cyber security and thus continue to gain in importance.

[18] NATO CCD COE, Definition, https://ccdcoe.org/cyber-definitions.html.



3. The protagonists in the provision of national cyber security

Which institutions at state level have which responsibility and tasks for cyber security?

The configuration of the individual institutions at the national level in the cyber area differs from state to state. In contrast to foreign or defense policy, there are no uniform structures in the countries examined, which are reflected, for example, in a single ministry with a leading area of responsibility. Cyberspace, which is difficult to define, once more displays its special and complex nature here, since it is not so easy to grasp and thus assign to other policy areas in terms of subject matter and organization.

It is therefore no surprise that the respective national cyber strategies normally designate several protagonists responsible for cyber security at the state level. It is evident that "Cyber" as a topic is assigned to more than one portfolio in the various states. Thus this interdisciplinary topic is assigned, depending on the focus, to individual ministries, for example cyber crime to the Department of the Interior, cyber foreign policy to the State Department and cyber defense to the Department of Defense.

„There are few areas where internal and external security are as closely intertwined as they are in cyber space. The threat situation in cyber space necessitates a holistic approach in the framework of cyber security policy. Ensuring cyber security and defence is therefore a whole-of-government task that must be performed collectively. This includes the joint protection of critical infrastructure. The tasks to be carried out are specified in the Cyber Security Strategy, which is developed under the direction of the Federal Ministry of the Interior. Defence aspects of national cyber security are core tasks of the Federal Ministry of Defence and the Bundeswehr, while overall responsibility for international cyber security policy lies with the Federal Foreign Office."

(Germany, White Paper 2016)

All in all, the coordinating institutions vary from state to state when it comes to cyber issues. In most cases, however, one ministry is entrusted with the lead. In the Turkish context, for example, this role falls to the Ministry of Transport, Marine and Communications, which apart from drawing up the National Cyber Security Strategy also coordinates the Cyber Action Plan for 2016-2019.

In Germany – despite an existing division of tasks – the Federal Ministry of the Interior Federal Ministry of the Interior, Building and Community is taking the lead in state cyber issues. In Ireland, too, one Ministry, the Ministry of Communications, Energy and Natural Resources, takes on this function and controls cyber policy through the National Cyber Security Centre located there.

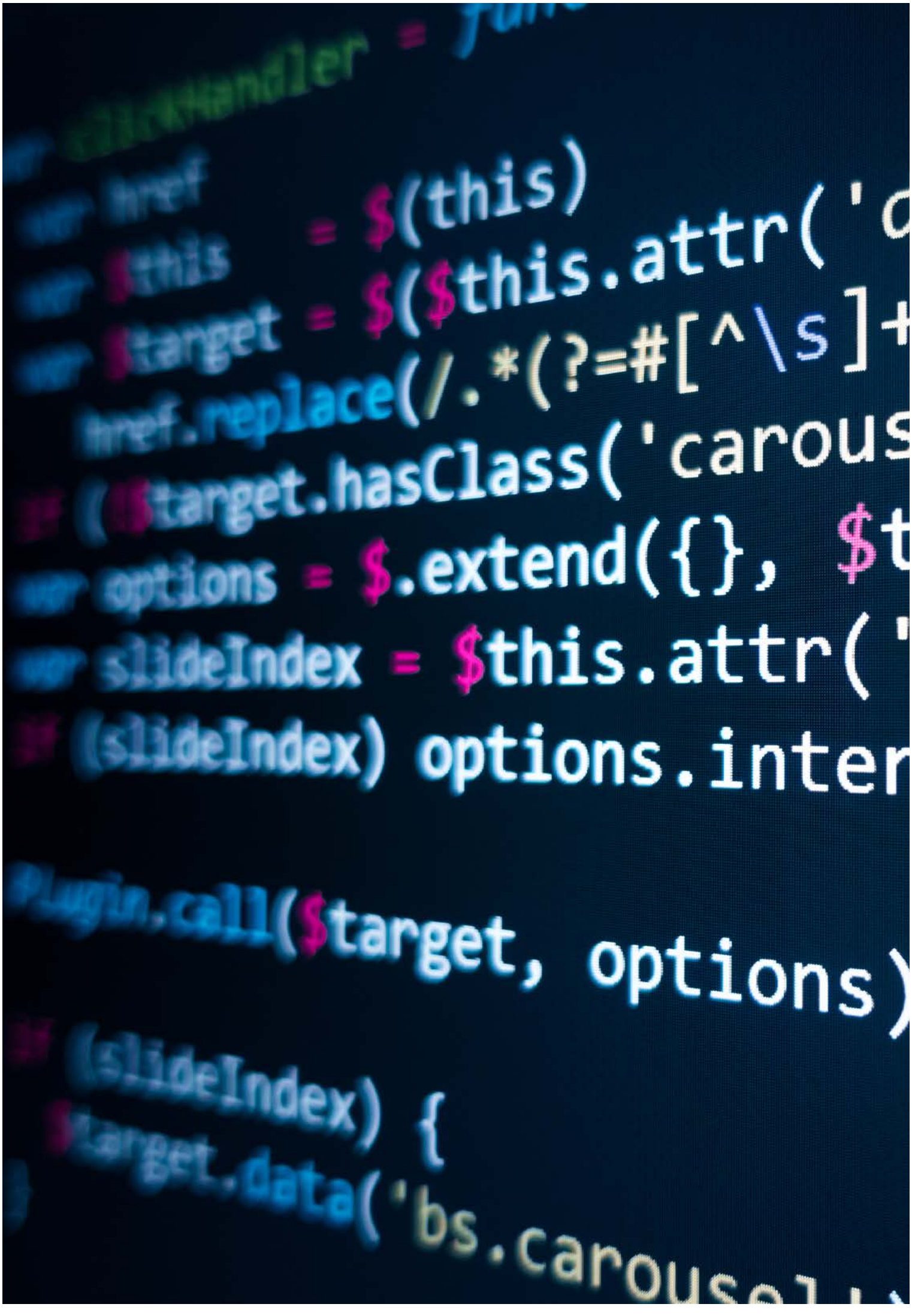
The basic number of institutions mentioned in the respective national cyber strategies varies greatly in some cases. For example, some strategies mention three or fewer protagonists (e.g., Lithuania, Poland or Portugal); for other countries the figure is even in double figures (e.g., Latvia). Germany is also one of the countries whose cyber landscape is comparatively differentiated. Thus, apart from the Federal Office for Information Security (BSI) and the Cyber and Information Domain Command (KdoCIR), there are other institutions such as the National Cyber Defense Centre (NCAZ) or the Central Office for Information Technology in the Security Sphere (ZITiS).

In some cyber security strategies, it is even very difficult to recognize a clear division of responsibilities at the State level. Thus in the Lithuanian strategy, for example, just one actor is named, the CERT-LT. Based on this, however, it can be said that these Computer Emergency Response Teams (CERT) are almost an integral part of cyber security in European countries: CERT/CSIRT structures and their funding are named in just around three quarters (19 out of 29) of the national cyber security strategies under review. This is also the case in Germany, where the Federal Computer Emergency Response Team (CERT-Bund) was formed in 2001. A group of security experts support state institutions in solving specific IT security incidents. Further independent CERT structures are established in other federal authorities, in federal state administrations, in individual companies, and in scientific institutions. Apart from CERT-Bund, there is also the Bundeswehr's Computer Emergency Response Team (CERTBw), which protects the Bundeswehr's approximately 200,000 computers from attacks emanating from the internet.

In recent years, a tendency has also emerged that more and more European states increasingly understand cyberspace as a place of potential warfare and are taking steps in this respect. This is also in line with developments at the international organization level, for example with NATO defining cyberspace as an independent warfare domain in 2016. In recent years, many states have established military cyber capabilities in their armed forces in order to be prepared for "cyber war" in an emergency. This includes the Federal Republic of Germany, which officially set up the Cyber and Information Space organizational unit within the Bundeswehr for this purpose in April 2017. Apart from Germany, Bulgaria, Finland, the United Kingdom, Ireland, Latvia, Poland and Spain have written military cyber defense capacities into their national cyber security strategies, which represents nearly one-third of the strategies considered. Denmark, Germany, the United Kingdom, Norway, Spain, and the United States are also working together until early 2019 to establish principles of cyber warfare intended to guide their individual armed forces in the use of cyber operations.[19] The major European states such as Germany, France, and the United Kingdom above all have invested in military cyber capacity in recent years.[20]

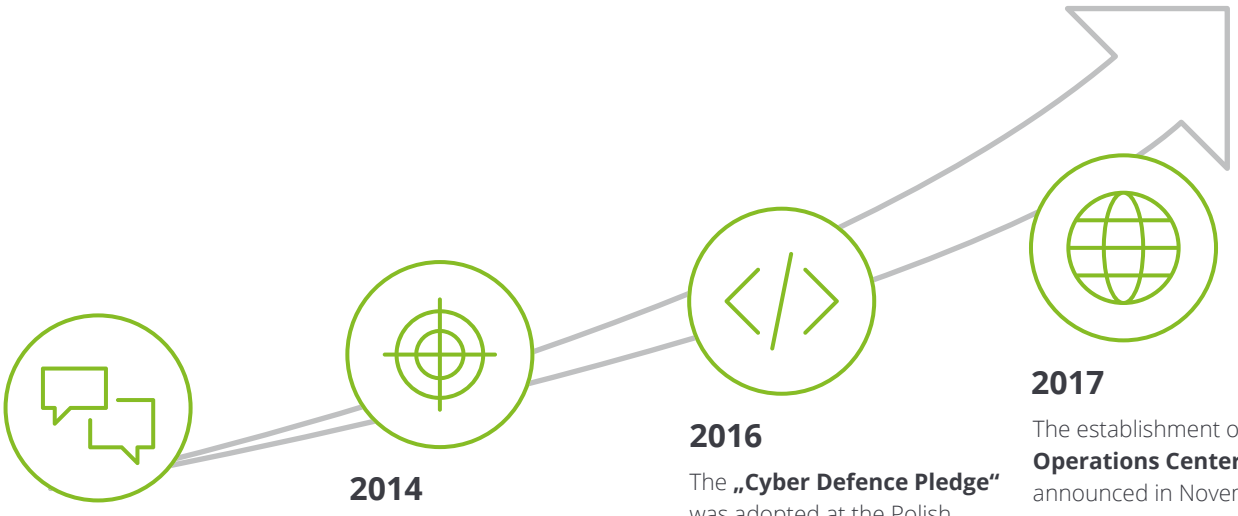
[19] https://www.reuters.com/article/us-naato-cyber/nato-mulls-offensive-defense-with-cyber-warfare-rules-idUSKBN1DU1G4?utm_source=applenews

[20] https://www.euractiv.de/section/eu-innenpolitik/news/eu-ruesten-fuer-den-cyberkrieg/


$(this)
$($this.attr('
href.replace(/.*(?=#[^\s]+
($target.hasClass('carous
options = $.extend({}, $t
slideIndex = $this.attr('
(slideIndex) options.inter
Plugin.call($target, options)
(slideIndex) {
$target.data('bs.carousel')

4. Status of international cooperation on defense against cyber threats

Fig. 9 – NATO – International cooperations for cyber defense



2010

Cyber defense is mentioned in the Strategic Concept among the threats to NATO.

2014

The **„Enhanced NATO Policy on Cyber Defence“** was adopted at the Wales summit.

2016

The **„Cyber Defence Pledge“** was adopted at the Polish summit.

Cyber was named as an independent Warfare Domain.

A cyber attack is named as a possible trigger for a collective defense case.

2017

The establishment of a **Cyber Operations Center** was announced in November.

NATO: Cyber defense has reached the top of the agenda

At the latest since the cyber attacks against state authorities and companies in NATO member Estonia in 2007, the Alliance has gradually upgraded the issue of cyber defense and taken measures in this respect. The increasing threat of cyber attacks was already pointed out in the 2010 Strategic Concept. However, a decisive turning point on the part of the member states was the adoption of NATO's "Enhanced Cyber Defence Policy" at the 2014 summit in Wales. This provides for cyber attacks to be seen in the context of 'collective self-defense' and that such operations on a Member State can also lead to the declaration of a 'collective defense case for the alliance' (Article 5 of the NATO Treaty) in an emergency. Cyber defense was also linked to Article 3 (Member States' responsibility for their own security) and Article 4 (possibility of consultation within NATO).

A further upgrading took place at the NATO summit in Warsaw in 2016, when the former 28 member states adopted the "Cyber Defence Pledge" and also defined the cyberspace as the fifth operational domain (in addition to land, air, sea, and space). It contains seven – albeit non-binding – objectives for its members, including the treatment of cyber defense at the highest national strategic level and the promotion of training activities in the individual countries. The first report on the implementation of these seven objectives in each member state was presented at the NATO Heads of State and Government meeting in May 2017.

„[W]hilst in many Allies the cyber defense policy framework was relatively mature, challenges existed in both resourcing, recruitment, and retention."[21]

(Robertson, Neil, NATO Policy Officer, Cyber Defense at NATO: From Wales to Warsaw, and Beyond, in: Turkish Policy Quarterly, Fall 2017)

„Cyber attacks can be as dangerous as conventional attacks. They can shut down important infrastructure. They can have a great negative impact on our operations."

(Jens Stoltenberg, NATO Secretary General,2014; in: Turkish Policy Quarterly 2017)

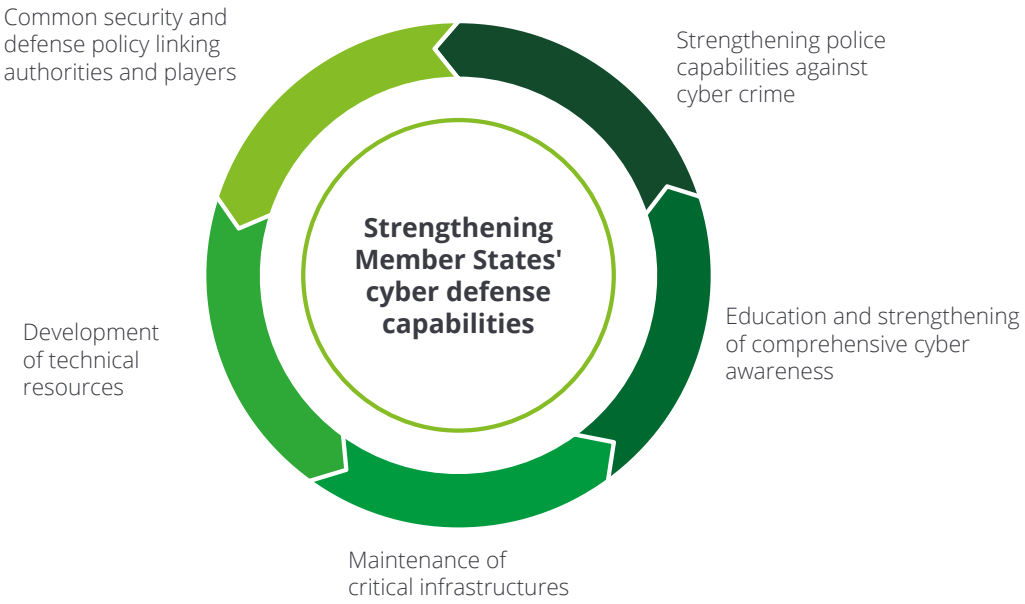
[21] http://turkishpolicy.com/article/887/cyber-defense-at-nato-from-wales-to-warsaw-and-beyond

A further step followed in November 2017 when NATO announced the establishment of a Cyber Operations Center. The objective of the center is to be anticipating threats more rapidly and increasing the ability to respond. Individual cyber units can now also be integrated into Alliance operations and missions. The capabilities will be initially expected to be made available on a voluntary basis by the Member States. However, it has not yet become clear to what extent the Center and NATO also regard offensive cyber operations as part of their field of activity.

Furthermore, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn is an institution whose task is to increase cooperation between NATO and its member and partner states with regard to cyber defense through training, consulting, research and development. The CCDCOE also prepared the Tallinn Manual 2.0, which is perhaps the most detailed document linking international law and cyberspace. The Tallinn Manual 2.0 is a legal analysis of frequently occurring cyber incidents that states are confronted with on a daily basis and that are characterized by the use of violence and armed conflict. Version 2.0 completes the original content of the Tallinn Manual. It primarily covers violations of the prohibition of violence in international relations by means of severe cyber operations. However, it is not binding in nature.

In addition, the Cyber Coalition is an annual NATO exercise in which the various member states test their capabilities and practice international cooperation in the area. The CCDCOE also hosts the annual cyber exercise Locked Shields, in which states, universities, and large companies participate in a real-time simulation. At the EU level, EU CYBRID was also held in Tallinn in September 2017, with the participation of Defense Ministers, to test decision-making ability in the face of cyber and hybrid threats.

Fig. 10 – European Union – Multi-level cyber security



EU: Cyber security on multiple levels

The issue of cyber security has also gradually gained in importance for the European Union (EU). The first milestone here was the publication of the European Union's Cyber Security Strategy in 2013. One of the core messages of the strategy is that although the EU is basically dealing with the issue, both conceptually and through its own sub-organizations, those primarily responsible for preventing and responding to cyber attacks are the individual Member States at the national level. This strategy was updated in September 2017 to include further aspects such as the further development of the European Network and Information Security Agency (ENISA) into an EU agency for cyber security, the expansion of a European crisis management mechanism, and the development of projects in the field of military cyber defense. Furthermore, in October 2017 the EU adopted a diplomatic response framework to deal with possible cyber incidents. For the time being, however, this only includes non-military means.[22]

In addition to the Cyber Security Strategy, other strategy and concept papers also address cyber security, including the Digital Agenda for Europe 2020, the EU's Global Strategy for Foreign and Security Policy, or the Common Framework for Combating Hybrid Threats.

[22] https://www.swp-berlin.org/publikation/die-eu-als-friedensmacht-in-der-internationalen-cyberdiplomatie/

The main organizations dealing with cyber security within the EU are, apart from the currently understaffed ENISA, the European Commission, the EU's Computer Emergency Response Team (CERT-EU) and the European Public-Private Partnership for Resilience (EP3R). Other relevant protagonists are the EU Intelligence and Situation Centre (EU INTCEN) and the Hybrid Fusion Cell embedded at INTCEN, which deals with the analysis of hybrid threats. The European Cyber Crime Centre (EC3) and EUROPOL are the basic protagonists in the fight against cyber crime.

In addition, the Network and Information Systems Directive (NIS Directive), which came into force in August 2016, established a framework for EU-wide rules on cyber security. The Directive requires Member States to take protective measures against cyber attacks, including the establishment of National Contact Points and Computer Security Incident Response Teams (CSIRT) and the establishment of security and notification requirements for critical infrastructure operators.

„Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."

(Cybersecurity Strategy of the European Union, 2013)

Tab. 1 – European Union – Areas of competence cyber defense and diplomacy

Cyber security in the EU[23]	Peace, Security, Justice	Single Market	Common Security and Defense Policy: Cyber Defense	Common Foreign and Security Policy: Cyber Diplomacy
European Union	Europol (EC3) Eurojust EU-LISA	ENISA CSIRT Network CERT EU	EDA GSA	EEAS SIAC (EU INTCEN, EUMS INT) EU SITROOM EU-Hybrid Fusion Cell ERCC
National level	Executive and data protection authorities	Competent authorities for NIS National CSIRTs	Defense, military and security authorities	Foreign ministries

[23] Dr. Bendiek, A. (2018): Die EU als Friedensmacht in der internationalen Cyberdiplomatie, SWP-Aktuell 22, p. 4.

EU and NATO: Planned cyber security cooperation is making slow progress

In a "Joint Declaration" in June 2016, both organizations declared their intention to cooperate more closely. They also want to act together in the fight against cyber attacks, among other things by sharing EU and NATO approaches to cyber defense and ensuring interoperability of requirements and standards in this area. Training courses are also to be open to employees of the other organization. Furthermore, research and technological innovation should also be encouraged between the two protagonists, as should joint participation in cyber exercises.

In the same year, the EU and NATO adopted a Technical Agreement which provides for the exchange of technical information between the EU's Computer Emergency Response Team (CERT-EU) and the NATO Computer Incident Response Capability (NCIRC).

Nonetheless, cooperation between the two organizations is inhibited by higher-level problems, in the fight against cyber crime too. The specific separate lives of the two organizations and the unresolved Cyprus conflict play an obstructive role here.

Cyber security and the UN: Is the desire for international cyber standards still sustainable?

With increasing digital networking and the global impact of cyber attacks, states have taken up the challenge of creating international cyber norms. The main framework for this objective was until recently the UN Group of Governmental Experts (UN GGE[24]), which has dealt with this issue in five rounds of negotiations since 2004. The format consists of 25 experts nominated by the individual members. An initial breakthrough was achieved in 2013, when the UN GGE adopted a consensus report confirming the application of international law to cyberspace.

However, the most recent GGE round, in 2016/2017, was marked by disillusionment: the members could not agree on a new consensus report, as the crucial question of how international law should be applied to cyberspace turned out to be the greatest point of contention between Western states on the one hand and Russia and China on the other.

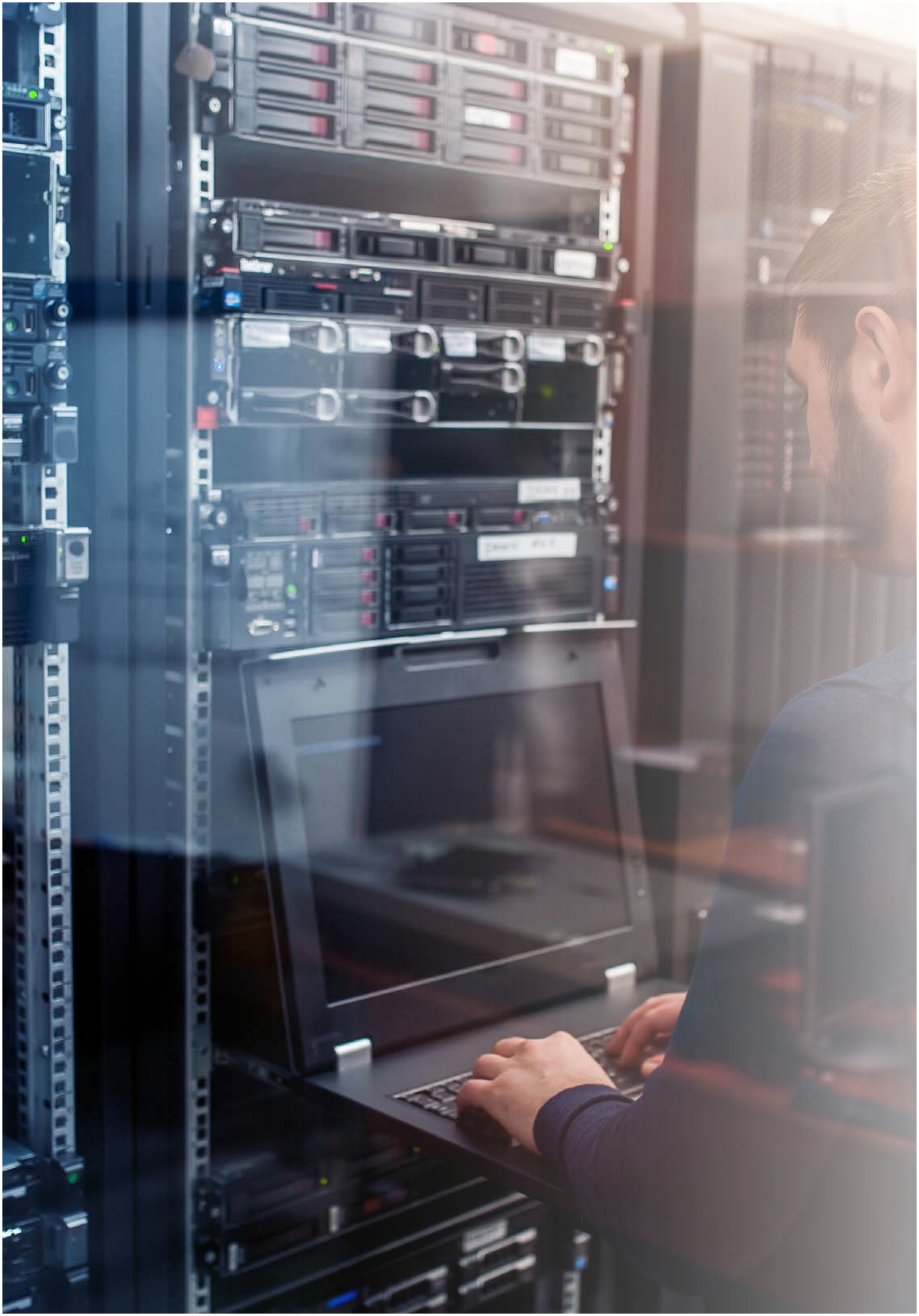
Thus it remains to be seen whether this format for creating standards will continue to exist or whether the individual states will open up new possibilities for cross-border understanding in cyberspace. Accordingly, increased reliance is being placed on bilateral or trilateral cyber consultations between states such as, for example, the United States and Germany.

Apart from the UN GGE, numerous other agencies and institutions, such as the UN Office on Drugs and Crime (UNODC), the UN Interregional Crime and Justice Research Institute (UNICRI), and the UN Institute for Disarmament Research (UNIDIR), are also addressing cyber issues. However, this is only a sub-section of the protagonists in the UN area of responsibility, as can be seen from various resolutions of the UN General Assembly.

Fig. 11 – International cooperation is predominantly a core objective in national cyber security strategies

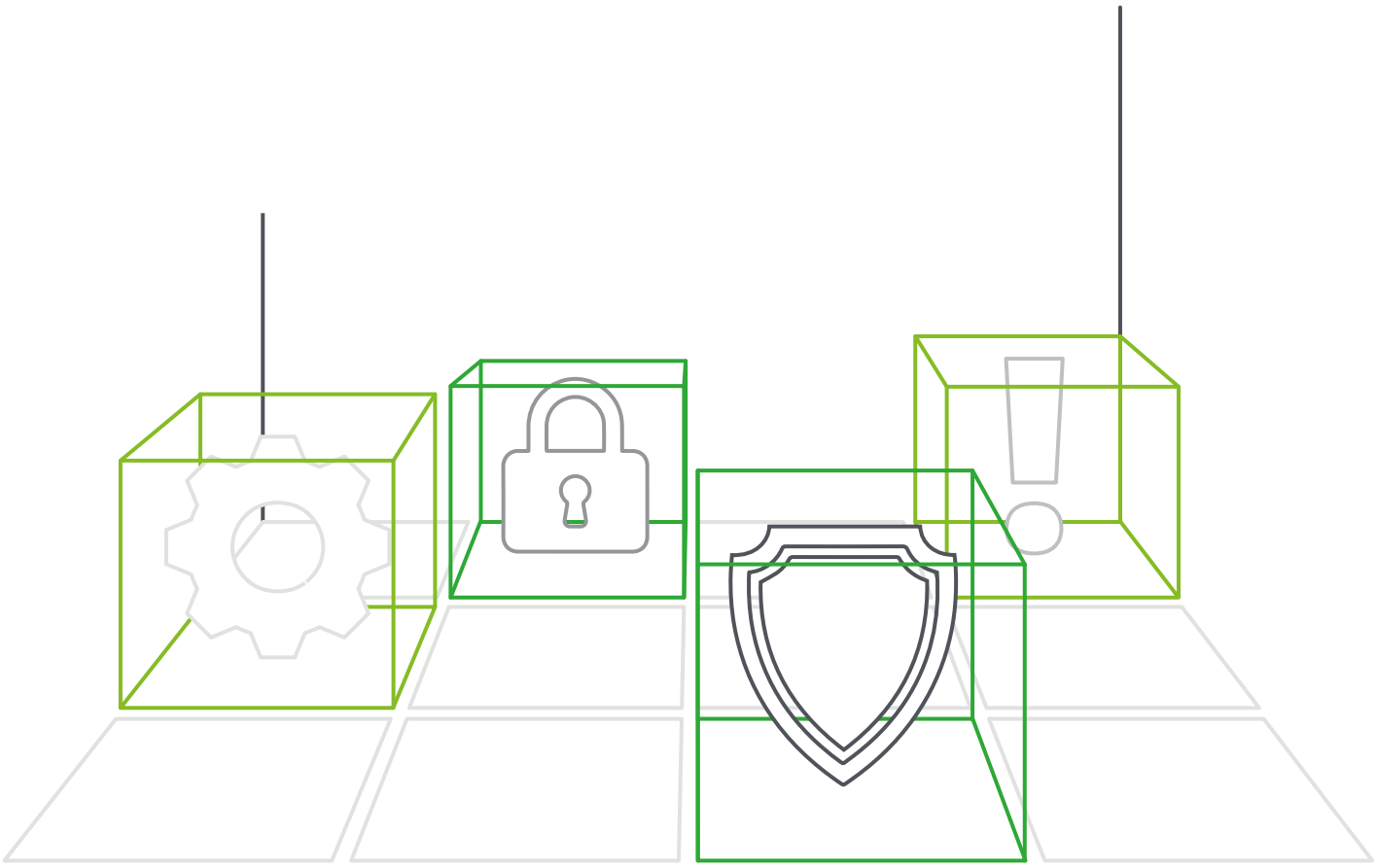
17 out of 29 strategies
focus on international cooperation for the exchange of knowledge and rapid prosecution; these should be both public and public-private partnerships.

[24] UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security.



5. Fields of action

Our systematic comparison has identified six possible fields of action. We are convinced that they will play a major role when national cyber security strategies are updated.



1. Updating older strategies

States, criminal groups, and individual hackers are constantly honing their "cyber weapons" so that the cyber threat situation is changing at a rapid pace. Above all, the trend towards cyber becoming a new operational area of warfare is clearly identifiable. The associated NATO resolution in 2014 was the clearest sign of this. We assume that European states with older strategies will conduct a new internal discourse in order to adapt to the new situation and draw new concepts or strategies. They will closely coordinate national cyber security strategies with national security strategies and adapt them in the same change process in future. European countries' national strategies will increasingly need a common European strategic framework.

2. Support for and dynamization of strategy formulation with the help of trend and scenario analyses

Trend and scenario analyses would appear to be a suitable tool to deal with the prevailing uncertainties in cyberspace and to anticipate them as best as can be. On the one hand, they can be used to identify and quantify long-term developments. On the other hand, parameters whose future development is uncertain, but to which a significant influence on cyber security is ascribed, can be included in the strategy.

The perception of the threat situation and responsibility underlying the strategies could be reviewed at regular intervals or on a permanent basis. We believe that this will establish dynamic processes for adapting cyber security strategies. They could involve the Cyber Incident Reporting Centers up to the level of government enforcement and enable those responsible to respond quickly to changes in the cyber threat situation and to act in the interests of anticipatory protection of their society and economy. An interruption in the discussion of a strategy after its entry into force until the next update would thus not occur.

3. Agreement on uniform definitions at the international level

We believe that greater efforts will be needed in future to establish uniform definitions in order to permit effective cooperation at the international level. This would permit common and possibly binding cyber security standards to be created. It would considerably sharpen and strengthen cooperation and the ability to react jointly. Among other things, guidelines for combating cyber attacks could be defined.

4. Clear definition of responsibility

Since cyberspace, which is difficult to define, is not so easy to grasp spatially, thematically, and organizationally compared to other policy areas, the corresponding area of responsibility in the individual European states is often distributed over several ministries and institutions. We believe that in future there will be increased efforts to clearly attribute responsibilities and that a partial modification of the established state security structures and the underlying legal framework will thus be achieved.

5. Active cyber defense to reinforce cyber security

As part of our analysis of the strategies, we have found that the question of the effectiveness and appropriateness of offensive measures – preventive or reactive – is currently being discussed intensively and controversially in the context of cyber defense (active cyber defense).

One aspect of the discussion is the question of whether preventive measures can increase the effort and costs of a potential attacker and thus ultimately reduce the risk of a cyber attack. Also discussed is the question of the capabilities required to force a potential attacker to abandon their project, or the use of conventional means of effective defense in cyber attacks.

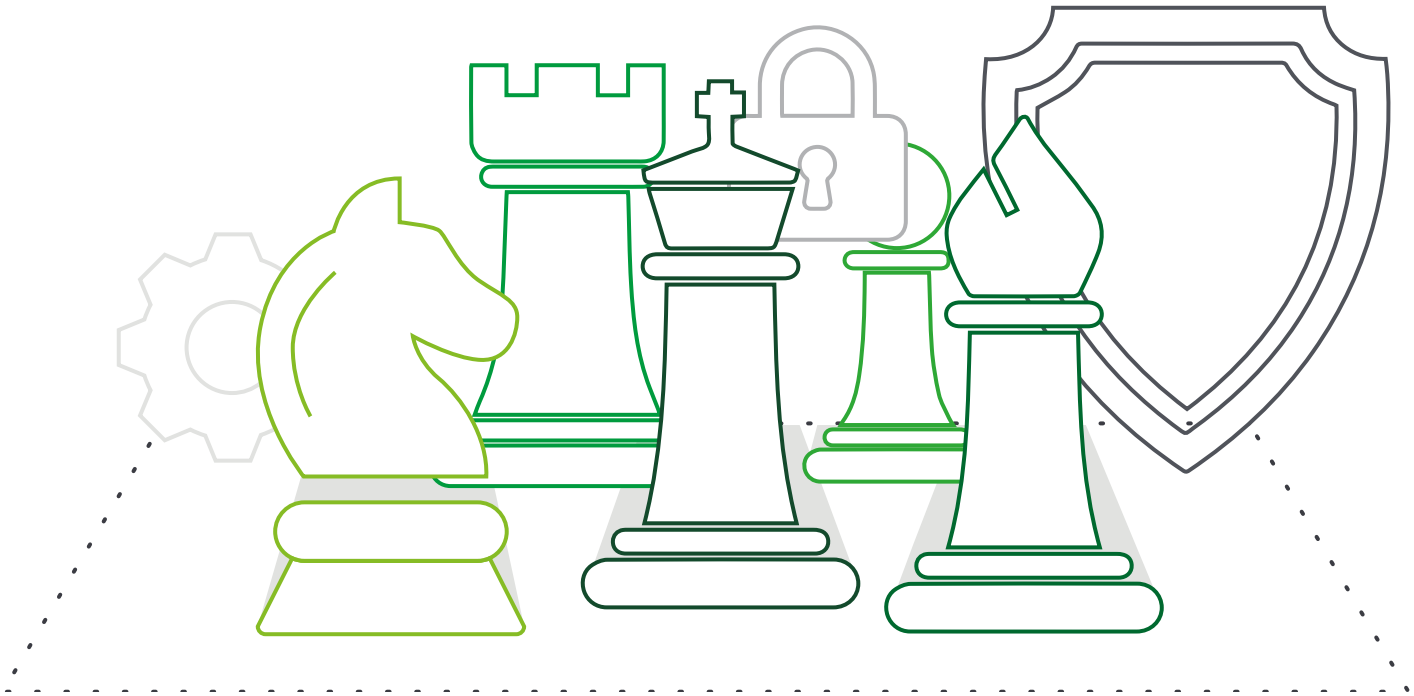
We are convinced that in the future, statements on the use, legality and effectiveness of Active Cyber Defense will play an important role in national strategies.

6. Establishment of an international exchange platform and joint exercises

Owing to uncertainty and – compared to other phenomena – less experience with regard to cyberspace, we are convinced that states will continue to pool their knowledge and expertise on current trends and possible cyber attacks. They will create a common knowledge base, share best practices, and strengthen institutions such as NATO and the EU, as well as bilateral cooperation. Since cyberspace is difficult to define and brings with it immense uncertainty regarding the nature of security-relevant parameters, exercises involving EU and NATO states appear to be important in order to gain a common feeling for a rapid response capability and appropriate response options. By simulating specific scenarios and actions, options for certain situations could be developed in advance so that they are at hand in an emergency. We believe that an exchange platform and joint exercises will uncover certain differences in approach that will serve as a basis for discussion and will contribute to joint solutions.

Within the fields of action, decision-makers should involve all stakeholders from politics, the military, intelligence services, network operators, business, and civil society in a comprehensive cyber security strategy. Close cooperation, both nationally and internationally, with all parties involved in the field of cyber security is an indispensable precondition to repel professional attacks equally professionally.

6. National and international cyber security strategies at a glance



Austria

Ranking of cyber threats versus other national threats (NSS)

Listed along with international terrorism, weapons of mass destruction, national and international conflicts, resource scarcity, organized crime, migration, and economic crises.

National Cyber Security Strategy (NCSS)

Publication: 2013
Published by: Federal Chancellery
Timeframe: n.n.
Core objectives:
- creating a secure cyberspace for data exchange
- development of a resilient infrastructure against cyber threats
- raising awareness and promoting new initiatives in national cyber security dialogues
- expansion of necessary ICT infrastructures
- developing a stronger legal framework to simplify international prosecutions
- protection of interests at national and local level
- promotion of public-private cooperation
- protection of the identity and privacy of citizens

Cyber threats described:
- identity fraud
- misuse of the internet for extremist purposes

Main protagonists:
public
- Government Computer Emergency Response Team (GovCERT.at)
- Cyber Security Steering Group
- Cyber Crime Competence Center (C4)

military
- Military Cyber Emergency Readiness Team (MilCERT)
- Federal Ministry of Defense (BMLV)

Belgium

Ranking of cyber threats versus other national threats (NSS)

Are considered serious threats to national security.

National Cyber Security Strategy (NCSS)

Publication: 2012
Published by: Prime Minister
Timeframe: n.n.
Core objectives:
- creating a secure cyberspace
- guaranteeing fundamental rights and values
- expanding security measures
- protecting crucial infrastructures
- developing an independent cyber security policy
- expanding partnerships and cooperation
- investing in education and research

Cyber threats described:
- botnets
- cyber espionage
- cyber warfare
- cyber terrorism

Main protagonists:
public
- Computer Emergency Response Team (CERT.be)
- Commission for the Protection of Privacy (CPP)
- National Cyber Security Center (NCSC)
- The Belgian Federal Computer Crime Unit (FCCU)
- Federal Public Service Information and Communication Technology (Fedict)
- Security of the State: Veiligheid van de Staat (VSSE)

military
n.n.

Bulgaria

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2016
Published by: Regional Cybersecurity Forum, National Cybersecurity Coordinator
Timeframe: 2016-2020
Core objectives:

- expanding the national cyber security system
- improved coordination of response to cyber threats
- development of crucial infrastructures
- collaboration between government and operators
- formation of international coalitions for the exchange of information

Cyber threats described:

n.n.

Main protagonists:

public

- National Cyber Situational Center
- Computer Emergency Response Team (CERT.bg)
- Cyber Crime Center

military

- Military Cyber and Information Center (Mil CiRC)

China

Ranking of cyber threats versus other national threats (NSS)

No information

National Cyber Security Strategy (NCSS)

Publication: 2016
Published by: 12th National People's Congress
Timeframe: n.n.
Core objectives:

- respect for the constitution and its fundamental rights
- maintenance of national interests such as public security and social welfare
- maintaining cyber sovereignty

Cyber threats described:

- identity theft and loss of personal data
- computer viruses, network attacks, malware
- data manipulation and use by third parties
- illegal data trading and transmission of legally protected data
- trafficking in cyber crime hardware

Main protagonists:

n.n.

Croatia

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2015
Published by: n.n.
Timeframe: n.n.
Core objectives:

- ensuring secure data transfer
- creation of a reliable and resilient cyberspace
- developing the national criminal justice system
- measures to raise awareness among cyberspace users, legal entities, individuals, and the public
- public education through educational programmes
- development and research of new technologies
- internationally coordinated exchange of knowledge and information

Cyber threats described:

n.n.

Main protagonists:

public

- National Cyber Security Council
- Operational and Technical Cyber Security Coordination Group
- Computer Emergency Response Team (CERT)

military

n.n.

Czech Republic

Ranking of cyber threats versus other national threats (NSS)

Listed along with a series of human failures and environmental disasters.

National Cyber Security Strategy (NCSS)

Publication: 2015
Published by: National Cyber Security Centre of National Security Authorities
Timeframe: 2015-2020
Core objectives:

- development of relevant infrastructures
- cooperation between national and international authorities
- ensuring protection of nationally relevant information networks and infrastructures
- promotion of cooperation in the public-private sector
- strengthening consumer confidence in the population
- information and sensitization through public education
- strengthening research and development
- improving national law enforcement

Cyber threats described:

- cyber espionage
- organized crime
- dissemination of false information against state institutions
- cyber terrorism
- malware, data theft

Main protagonists:

public

- National Cyber Security Centre (NCSC)
- Computer Emergency Response Team (CERT.cz)
- National Security Authority (NSA)

military

n.n.

Denmark

Ranking of cyber threats versus other national threats (NSS)
Named along with militant Islamism, terrorism, migration flows and climate change.

National Cyber Security Strategy (NCSS)

Publication: 2018
Published by: Danish Government
Timeframe: 2018-2021
Core objectives:
- extending the information security of critical sectors in the economy and the public
- strengthening robust digital infrastructures and technologies
- further training and education of the population
- improved cooperation between public-private partnerships

Cyber threats described:
- data theft
- attacks on public institutions and crucial infrastructure
- cyber espionage, cyber sabotage, cyber crime
- cyber warfare, terrorism
- malware, ransomware

Main protagonists:
public
- Danish Centre for Cyber Security
- Central Operational Communication Staff (DCOK)
- National Operative Staff (NOST)
- Government Security Committee
- Agency for Digitization
- Danish Security and Intelligence Services

military
n.n.

Estonia

Ranking of cyber threats versus other national threats (NSS)
Named along with economic instability, radicalization, terrorism, organized crime, corruption, migration flows and a variety of other emergencies.

National Cyber Security Strategy (NCSS)

Publication: 2014
Published by: Ministry of Economic Affairs and Communication
Timeframe: 2014-2017
Core objectives:
- raising national awareness of cyber threats
- protection of information systems
- improved combat of cyber crime
- development of a national cyber defense
- promoting cross-sector cooperation

Cyber threats described:
- cyber crime
- dependence on ICT infrastructures and electronic services

Main protagonists:
public
- Estonian Information System Authority (RIA)
- Department of Critical Information Infrastructure Protection (CIIP)
- Estonian Defence League's Cyber Unit (EDL CU)

military
n.n.

Finland

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2013
Published by: Secretariat of the Security and Defence Committee
Timeframe: n.n.
Core objectives:

- model of cooperation between authorities and institutions
- ensuring public cyber security
- strengthening of existence-relevant infrastructures
- developing police and military capabilities
- participation in international organizations
- developing a legal framework for prosecution of crime

Cyber threats described:

n.n.

Main protagonists:

public

- Government Information Security Management Board (VAHTI)
- National Cyber Security Centre
- Finnish Communications Regulatory Authority (FICORA)
- Strategic Cyber Security Centre of Excellence (TIVIT)

military

- Military Cyber Defence Forces

France

Ranking of cyber threats versus other national threats (NSS)

In the 2008 and 2013 White Papers, cyber attacks are equated with terrorist attacks, weapons of mass destruction, natural and health crises, industrial accidents, attacks on the state and its citizens.

National Cyber Security Strategy (NCSS)

Publication: 2015
Published by: Prime Minister
Timeframe: n.n.
Core objectives:

- defense capability and security of state information systems and critical infrastructures
- safeguarding privacy, data protection, and cyberspace stability
- information, sensitization, and further training of the population
- building trust among the population
- expansion of digital business technologies

Cyber threats described:

- cyber espionage, malware
- data and identity theft
- blackmail, sabotage
- trading in illegal products

Main protagonists:

public

- National Cybersecurity Agency (ANSSI)
- Defence Procurement Agency (DGA)

military

- Cyber Defense Commando (COMCYBER/COCYBER)
- Cyber Defense Reserve

Germany

Ranking of cyber threats versus other national threats (NSS)
Named along with transnational terrorism, interstate conflicts, weapons of mass destruction, climate change, irregular migration, epidemics and pandemics, fragile states and governments, and security of supply for transport and trade routes.

National Cyber Security Strategy (NCSS)

Publication: 2016
Published by: Federal Ministry of the Interior, Building and Community
Timeframe: n.n.
Core objectives:
- secure and self-determined action of all citizens and industries
- efficient and sustainable national cyber security architecture
- promoting cooperation between government and industry
- formation of international cooperation and discussion platforms
- advancement and acquisition of technologies

Cyber threats described:
- data and identity theft
- attacks on public institutions and crucial infrastructure
- fake news, cyber espionage, cyber sabotage, cyber crime
- malware, ransomware, spam, botnets, side-channel attacks, drive-by exploits, exploit kits

Main protagonists:
public
- Federal Office for Information Security (BSI)
- Computer Emergency Response Team (CERT)
- Cyber Situation Center
- National Cyber Defence Centre (NCAZ)
- Central Office for Information Technology in the Security Sphere (ZITiS)

military
- Cyber and Information Domain Command (KdoCIR)

Greece

Ranking of cyber threats versus other national threats (NSS)
n.n.

National Cyber Security Strategy (NCSS)

Publication: 2017
Published by: n.n.
Timeframe: n.n.
Core objectives:
- improving general national online security
- maintaining reliable and fail-safe critical infrastructures
- securing confidential digital data transfer
- establishment and integration of secure and resilient cyberspaces
- optimization of cyber protectability
- institutional shielding of national cyber security frameworks
- promoting public cyber culture to protect citizens

Cyber threats described:
n.n.

Main protagonists:
- public and private actors are generally mentioned

Hungary

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2013
Published by: Prime Minister
Timeframe: n.n.
Core objectives:

- creation of public cyber-consciousness
- promotion of public institutions
- development of a secure cyberspace
- safeguarding national security
- development of efficient cyber skills
- protection of cyberspace and national databases
- quality assurance of IT and communications products and services
- quality assurance in education, research and development
- quality assurance of the cyberspace for children and future generations

Cyber threats described:

n.n.

Main protagonists:

public

- National Cyber Security Coordination Council
- Computer Emergency Response Team (EU CERT member)
- Sectoral Incident Response Centre

military

n.n.

Ireland

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2015
Published by: Department of Communications, Energy and Natural Resources
Timeframe: 2015-2017
Core objectives:

- developing resilient critical infrastructures in the public sector and key sectors of the economy
- comprehensive regulatory framework
- development of public administrative capacity
- information and sensitization of the population in dealing with data
- promotion of international cooperation

Cyber threats described:

- hacking, cyber crime, cyber espionage, data theft
- software and equipment failures caused by human errors, extreme weather events

Main protagonists:

public

- National Cyber Security Centre (NCSC)
- Computer Security Incident Response Team (CSIRT-IE)

military

- Cyber Defense Force (DF)

Italy

Ranking of cyber threats versus other national threats (NSS)
n.n.

National Cyber Security Strategy (NCSS)

Publication: 2013
Published by: Prime Minister of the Council of Ministers
Timeframe: n.n.
Core objectives:
- development of technical innovations
- increased cooperation between national institutions
- technical improvement of operational and analytical skills of all cyber institutions
- reinforcement of critical infrastructures
- raising security standards
- cooperation between public-private partnerships to protect national intellectual property
- educational programs to enhance security culture

Cyber threats described:
- cyber crime: data and identity theft, (internet) fraud
- cyber espionage: illegal acquisition of confidential data
- cyber terrorism: ideologically motivated intentions
- cyber warfare

Main protagonists:
public
- Agency for digital Italy
- Computer Emergency Response Team (CERT-SPC/PA)
- Department for Intelligence and Security (DIS)
- Committee for the Security of the Republic (CISR)
- National Anti-crime Computer Centre for the Protection of Critical Infrastructure (CNAIPIC)

military
n.n.

Latvia

Ranking of cyber threats versus other national threats (NSS)
n.n.

National Cyber Security Strategy (NCSS)

Publication: 2014
Published by: n.n.
Timeframe: 2014-2018
Core objectives:
- promotion of national and international cooperation
- educating the public, government institutions and private companies about the impact of their own activities and cyber threats
- simplified access to information and communications technologies for all citizens
- maintaining the rights and fundamental freedoms of individuals

Cyber threats described:
n.n.

Main protagonists:
public
- National Security Council for Information and Technology
- Ministry of Foreign Affairs (MFA)
- Financial and Capital Market Commission (FCMC)
- Ministry of the Interior (MoI)
- IT Computer Emergency Response Team (IT CERT.LV)
- Ministry of Education and Science (MoES)
- Safer Internet Centre of Latvia (Net.Safe)
- Constitution Protection Bureau (CPB)
- Ministry of Justice (MoJ) and Data State Inspectorate (DSI)

military
- Armed Forces (NAF) and Cyber Defense Unit (CDU)
- Ministry of Defence (MOD)

Lithuania

Ranking of cyber threats versus other national threats (NSS)
n.n.

National Cyber Security Strategy (NCSS)
Publication: 2011
Published by: Government of the Republic of Lithuania
Timeframe: 2011-2019
Core objectives:
- security of state information resources
- improved surveillance of electronic information systems
- development of the legal system
- securing critical infrastructures
- promotion of international cooperation
- information and sensitization of the population in dealing with data

Cyber threats described:
n.n.
Main protagonists:
public
- Computer Emergency Response Team (CERT.LT)

military
n.n.

Luxembourg

Ranking of cyber threats versus other national threats (NSS)
n.n.

National Cyber Security Strategy (NCSS)
Publication: 2018
Published by: Government Council
Timeframe: 2018-2020
Core objectives:
- strengthening public trust in the digital environment
- securing digital infrastructure
- promotion of the economy

Cyber threats described:
- ransomwares, DDOS, Brickerbot, BlackMail
- espionage, sabotage, cyber crime, data theft
- threat of business processes in companies

Main protagonists:
public
- Cybersecurity Board (CSB)
- High Commissioner for National Protection (HCPN)
- State's Information Technology Centre (CTIE)
- Governmental Computer Emergency Response Centre (GOVCERT)
- National Agency for the Security of Information Systems (ANSSI)
- Ministry of Defence
- Ministry of State, Media and Communication Unit
- State Intelligence Services
- Ministry of Economy
- National Centre for Cybersecurity Skills (C3)
- Coordination and Post-Incident Action Unit (CIRCL)
- Ministry of Foreign and European Affairs (MAEE)

military
- Luxembourg Army

Montenegro

Ranking of cyber threats versus other national threats (NSS)
n.n.

National Cyber Security Strategy (NCSS)
Publication: 2017
Published by: Ministry of Public Administration
Timeframe: 2018-2021
Core objectives:
- enhancement of cyber defense capability
- centralization of cyber know-how and resources
- securing critical infrastructures
- strengthening interinstitutional cooperation at regional and national level
- development of public-private partnerships
- education and sensitization in the population

Cyber threats described:
- cyber attacks, cyber warfare
- hacking, espionage, sabotage
- attacks by foreign governments, extremist and radical groups
- cyber terrorism, cyber crime
- human error and natural disasters

Main protagonists:
public
- Ministry of Public Administration within which the national CIRT operates
- National Security Agency
- Ministry of Interior / Police Administration
- Ministry of Justice
- Ministry of Education
- Directorate for Protection of Confidential Data

military
- Ministry of Defence / Army of Montenegro.

Netherlands

Ranking of cyber threats versus other national threats (NSS)
n.n.

National Cyber Security Strategy (NCSS)
Publication: 2018
Published by: National Coordinator for Security and Counterterrorism (Ministry of Justice and Security)
Timeframe: n.n.
Core objectives:
- building a resilient and reliable digital domain
- promoting a strong public-private partnership
- protection of vital interests
- resistance to cyber attacks
- combating cyber crime
- developing secure ICT products
- promoting cyber knowledge and skills
- formation of national and international coalitions

Cyber threats described:
- data and identity theft
- cybere spionage
- botnets, ransomware
- cyber-crime-as-a-service

Main protagonists:
public
- Joint Sigint Cyber Unit (JSCU)
- National Cyber Security Centre (NCSC)
- Security Operations Centre (SOC)
- Digital Trust Centre (DTC)
- Computer Emergency Response Team (CERT)

military
n.n.

Norway

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2017
Published by: The Ministry of Government Administration, Reform and Church Affairs
Timeframe: n.n.
Core objectives:

- defense against threats with an improved understanding of the situation
- rapid response in emergencies
- development of robust ICT infrastructures
- promotion of skills and abilities
- ensuring the protectability of information systems
- expansion of education and research programs for education

Cyber threats described:

- cyber espionage, cyber sabotage, cyber terrorism
- data and identity theft
- disloyal employees

Main protagonists:

public

- Norwegian National Safety Authority (NSM)
- Computer Emergency Response Team (NorCERT)
- Norwegian Postal and Telecommunications Authority (PT)
- Norwegian Center for Information Security (NorSIS)
- Norwegian Directorate of Civil Protection (DSB)
- Norwegian Intelligence Service (NIS)
- Norwegian Police Security Service (PST)
- Norwegian Data Protection Authority (DT)

military

n.n.

Poland

Ranking of cyber threats versus other national threats (NSS)

Named along with environmental disasters, attacks on critical infrastructures, and terrorism.

National Cyber Security Strategy (NCSS)

Publication: 2017
Published by: Ministry of Administration and Digitization, Internal Security Agency
Timeframe: 2017-2020
Core objectives:

- protection of information exchange between users of the Polish internet
- creation of a legal and organizational legal framework
- development, management, coordination, and security of cyberspace
- protection of crucial infrastructures

Cyber threats described:

n.n.

Main protagonists:

public

- Governmental Computer Security Incident Response Team (CERT.GOV.PL)

military

- Armed Forces and Departmental Centre for Security Management of ICT Networks and Services

Portugal

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2015
Published by: Prime Minister
Timeframe: n.n.
Core objectives:

- maintenance of fundamental rights and freedom of expression
- protection of citizens, their privacy and personal data
- development of cyberspace and crucial infrastructures
- sensitization of society
- free, safe, and efficient use of cyberspace for all strata of society

Cyber threats described:

- organized crime
- data and identity theft
- ideologically motivated attacks
- cyber espionage, cyber sabotage
- banking fraud

Main protagonists:

public

- National Centre for Cybersecurity (CNCS)
- Cyber Defence Centre (CCD)
- Computer Security Incident Response Team (CSIRT)
- Cyberspace Crisis Management Office

military

n.n.

Romania

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2013
Published by: Prime Minister
Timeframe: n.n.
Core objectives:

- adaptation of regulatory and institutional legal frameworks
- ensuring a secure and reliable cyberspace and its infrastructure
- promotion of national and international cooperation
- raising public awareness by developing a safety culture

Cyber threats described:

- threat to critical infrastructures from cyberspace
- cyber terrorism, cyber warfare, cyber crime, cyber espionage
- attacks by state and non-state actors
- access to and attacks on cyber infrastructures
- theft, deletion, damage to data
- harassment, extortion, pecuniary loss

Main protagonists:

public

- Supreme Council of National Defense
- National Cyber Security System (NSCC)
- Cyber Security Operative Council (COSC)
- Computer Emergency Response team (CERT-RO)

military

n.n.

Russia

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2014
Published by: Russian Government
Timeframe: 2014-2020
Core objectives:

- development of reliable and sustainable critical infrastructures, in peace and war
- promotion of national and international policy on cyber security and defense

Cyber threats described:

- information and communication technologies (information weapons)
- use of information technologies for terrorist purposes
- cyber crime
- disturbance of public order with information technologies
- anti-state propaganda

Main protagonists:

public

- Russian Security Council
- Ministry of Foreign Affairs
- Ministry of Communication
- Department of Justice

military

- Ministry of Defense

Slovakia

Ranking of cyber threats versus other national threats (NSS)

Listed along with international terrorism and weapons of mass destruction.

National Cyber Security Strategy (NCSS)

Publication: 2015
Published by: Prime Minister
Timeframe: 2015-2020
Core objectives:

- nationally protected and open cyberspace
- promoting trust among the population
- securing and developing critical infrastructures
- national programs promote exchanges between the private and academic sectors
- developing international cooperation to protect fundamental human rights and freedoms

Cyber threats described:

n.n.

Main protagonists:

public

- National Computer Emergency Response Team (CERT XY)
- Government Computer Emergency Response Team (government CERT)
- Ministry of the Interior
- Committee for Cyber Security
- Central State Authorities

military

n.n.

Slovenia

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2016
Published by: No information
Timeframe: 2016-2020
Core objectives:

- development of a comprehensive system for cyber defense
- development of a reliable infrastructure, without exception, for public and private institutions
- establishment of regulations
- safety of citizens and the economy
- operational guarantee of critical infrastructures
- combating and defense against cyber crime
- promotion of international cooperation

Cyber threats described:

- human errors
- digital piracy, abuse, blackmail, fraud
- dissemination of child pornography
- cybere spionage

Main protagonists:

public

- Slovenia National Computer Emergency Response Team (SI-CERT)
- Public Administration Computer Emergency Response Team (SIGOV-CERT)
- Slovenian Intelligence and Security Agency (SOVA)
- Agency for Electronic Communications Networks and Services of the Republic of Slovenia (AKOS)
- IT Directorate at the Ministry of Public Administration
- Centre for Computer Investigations with the capacities to combat cyber crime

military

- Ministry of Defence

Spain

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2013
Published by: Prime Minister
Timeframe: n.n.
Core objectives:

- safe use of information and telecommunications systems
- promoting the resilience of information technologies
- improvements in prevention and coordination skills
- sensitization of society
- development of skills, technologies
- strengthening international cooperation

Cyber threats described:

- hacking, sabotage, espionage
- terrorist organizations
- technically caused natural phenomena
- cyber crime

Main protagonists:

public

- Government Computer Emergency Response Team (Government CERT)
- Computer Emergency Response Team for Security and Industry (CERT)
- National Cryptology Centre (CCN-CERT)
- Spanish Public Administration System (SARA network)
- National Security Council
- Specialized cyber security committee
- Specialized Situation Committee

military

- Armed Forces Joint Cyber Defense Command (MCCD)

Sweden

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2017
Published by: Department of Justice
Timeframe: n.n.
Core objectives:

- cyber security strategy to defend against cyber attacks
- strengthening ICT infrastructures
- improve and manage networks, products, and system security
- improving skills, technologies, and expertise
- international cooperation in the fight against cyber crime

Cyber threats described:

n.n.

Main protagonists:

public

n.n.

military

n.n.

Turkey

Ranking of cyber threats versus other national threats (NSS)

n.n.

National Cyber Security Strategy (NCSS)

Publication: 2015
Published by: Ministry of Transport, Maritime Affairs and Communications (MoTMC)
Timeframe: 2016-2019
Core objectives:

- ensuring secure data transfer and protection in cyberspace
- security measures to minimize the effects of cyber attacks
- emergency plans to restore systems
- rapid criminal prosecution
- development of critical technologies at local level

Cyber threats described:

- information weapons
- use of information technologies for terrorist purposes
- cyber crime, phishing, warfare, malware, botnets
- disturbance of public order with information technologies
- anti-state propaganda
- network attacks, data manipulation and misuse

Main protagonists:

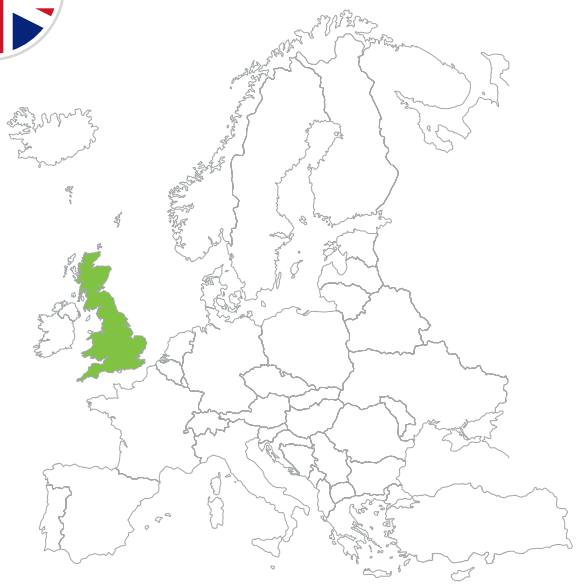
public

- Ministry of Transport, Maritime Affairs and Communication
- Ministry of Foreign Affairs (MoFA)
- Ministry of the Interior (MoI)
- Undersecretariat for Public Order and Security (UoPOS)
- National Intelligence Organization (NIO)
- Information and Communication Technologies Authority (ICTA)
- Scientific and Technological Research Council of Turkey (STRCoT)
- Financial Crimes Investigation Board
- Presidency of Telecommunication and Communication (PoTC)

military

- Turkish Armed Forces General Staff
- Ministry of National Defense (MoND)

United Kingdom



Ranking of cyber threats versus other national threats (NSS)
Named along with terrorism, military conflicts, public health, overseas instability, and major natural hazards.

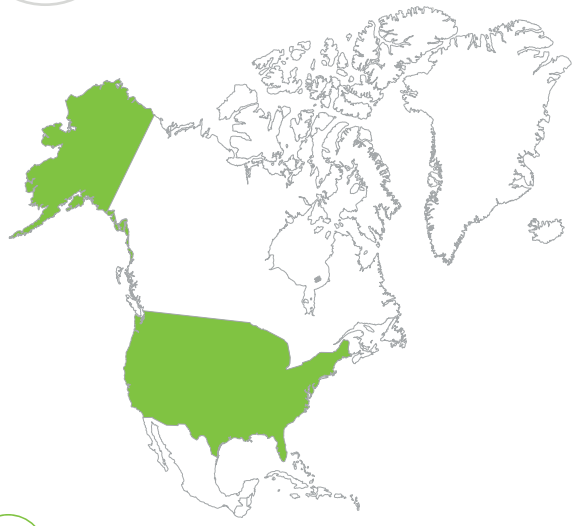
National Cyber Security Strategy (NCSS)
Publication: 2016
Published by: Her Majesty's Government
Timeframe: 2016-2021
Core objectives:
- rapid response to avert cyber attacks
- securing networks, data, and systems
- prosecution of criminals
- promotion of research and technology development
- expansion of international partnerships

Cyber threats described:
- cyber crime
- script kiddies
- cyber terrorism

Main protagonists:
public
- National Cyber Security Centre (NCSC)
- Government Communications Headquarters (GCHQ)
- National Crime Agency (NCA), National Cyber Crime Unit (NCCU)
- Government Digital Service (GDS)
- National Technical Authority for Information Assurance (CESG)
- National Computer Emergency Response Team (CERT-UK)

military
- Cyber Security Operations Centre (CSOC)
- Ministry of Defense (MoD)

United States of America (USA)



Ranking of cyber threats versus other national threats (NSS)
Named along with attacks on the homeland or critical infrastructures, threats to citizens abroad and allies, global economic crises and infectious diseases, climate change and weapons of mass destruction.

National Cyber Security Strategy (NCSS)
Publication: 2015
Published by: Department of Defense
Timeframe: 2015-2021
Core objectives:
- ensuring defense capabilities against cyber attacks
- creation and maintenance of cyber armed forces
- performing rapid response cyberspace operations
- securing defense information networks to protect the USA's vital interests
- promotion of international alliances and partnerships
- international stability and security

Cyber threats described:
- cyber attacks on Department of Defense networks
- data theft and destruction
- activist, ideologically motivated, and propaganda purposes
- cyber crime, especially against financial institutions

Main protagonists:
public
- Office of Cybersecurity and Communications (CS&C)
- National Cybersecurity and Communications Integration Center (NCCIC)

military
- United States Cyber Command (USCYBERCOM)
- Cyber Mission Force (CMF) of the Department of Defense (DoD)
- Military Departments Computer Emergency Response Teams (CERT)

European Union (EU)

Ranking of cyber threats versus other threats

No direct comparisons made. An ENISA study compares cyber threats against the EU with natural environmental disasters, inter-state conflicts, economic crises, CBRN attacks.

Cyber Security Strategy

Publication: 2013
Published by: European Commission
Timeframe: n.n.
Core objectives:

- developing the cyber defense capabilities of all member states
- Common Security and Defence Policy (CSDP)
- development of technical resources
- reducing cyber crime through international cooperation

Cyber threats described:

- malware, ransomware, denial-of-service, exploit-kits
- phishing, spam, botnets, cyber espionage, intelligence leaks
- physical manipulation, insider threats
- data privacy breaches, identity theft

Main protagonists:

- European Network and Information Security Agency (ENISA)
- European Cybercrime Centre (EC3)
- Computer Emergency Response Team (CERT-EU)
- Network of competent authorities
- European Defence Agency (DFA)
- European Security and Defence College (ESDC)
- European Cybercrime Training and Education Group (ECTEG)

North Atlantic Treaty Organization (NATO)

Ranking of cyber threats versus other threats

n.n.

Cyber Security Strategy

Publication: 2016
Published by: NATO
Timeframe: n.n.
Core objectives:

- collective defense through improved exchange of information and mutual support between allies
- protection of like interests and internationally applicable law in cyberspace
- intensification of cooperation with the European Union and industry

Cyber threats described:

No information

Hauptakteure:

- NATO Computer Incident Response Capability (NCIRC)
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
- NATO Communications and Information Systems School (NCISS)
- Cyber Defence Committee
- NATO Industry Cyber Partnership (NICP)

Ansprechpartner

Katrin Rohmann
Partner | Government &
Public Services Industry Leader
Tel: +49 (0)30 2546 8127
krohmann@deloitte.de

Peter J. Wirnsperger
Partner | Cyber Risk Leader
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Autoren

Knut Schönfelder
Senior Manager | Cyber Risk
Tel: +49 (0)40 32080 4447
kschoenfelder@deloitte.de

André Roosen
Manager | Cyber Risk
Tel: +49 (0)30 2546 8327
aroosen@deloitte.de

Kaan Sahin
Consultant | Cyber Risk
Tel: +49 (0)30 2546 85245
ksahin@deloitte.de

Deloitte.

Issue 10/2018