A Survey on National Cyber Emergency Plans

Konstantinos Adamos[1,2], Ioannis Filippopoulos[1], George Stergiopoulos[1] and Dimitris Gritzalis[2]

[1] Dept. of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece

[2] Dept. of Informatics, Athens University of Economics and Business, Athens, Greece

kadamos@aegean.gr
icsdm320027@icsd.aegean.gr
g.stergiopoulos@aegean.gr
dgrit@aueb.gr

Abstract: Operators of Essential services (OESs) and Critical infrastructures (CIs), whether private companies or public organizations are going through a digital transformation to pace with the evolution of technology and to bring better services to customers and countries' citizens. Operational Technology (OT) systems like Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) used to control and monitor functions in such infrastructures are converging with Information Technology (IT) environments. This convergence has exposed infrastructures to new cyber risks. For this reason, EU Member States have been trying to build resilience against cyber-attacks to ensure the stable operation of their states. Several countries have established cybersecurity incident response procedures as well as steps or phases of response before, during, and after a cyber incident. The sum of these procedures and guidelines constitutes their national cyber emergency plans (NCEPs). Still, these NCEPs differ widely in their approaches. These differences manifest as both managerial, governmental, legal, and technical, creating a complex environment worldwide. In this paper, we gather four major NCEPs worldwide to analyze and compare them with prominent standards and industry guidelines in cybersecurity, like the ISO 27001 and NIST 800 series. We investigate NCEP approaches to building cyber resilience based on their response models, their involved entities, the cooperation between agencies and other countries, and their risk-based categorization for cyber incidents. We elaborate on their differences, potential issues and divergences and argue whether these plans can be combined to bridge potential weaknesses. We selected and surveyed four (4) cyber emergency plans from four (4) countries that are frequent targets of cyber-attacks and have long experience in managing and responding to cyber incidents.

Keywords: Cybersecurity**,** Critical Infrastructure, Incident Response, National Cyber Emergency Plan, Operational Technology, Information Technology

1. Introduction

Cyber-attacks against national CIs are on the rise for the past decade (Lohrmann, 2022) (Trend-Micro, 2022) and cyber warfare has intensified (Claridge, 2022) (Pearson & Bing, 2022). Countries try to cope with this trend by build resilience to cyber-attacks to protect their most vital assets. This procedure is formalized by establishing national cybersecurity strategies and national cyber emergency plans. A National Cyber Emergency Plan (NCEP) is a set of guidelines, methodologies, and practices (usually following specific standard guidelines) that are formally applied by countries to respond to significant cyber incidents. In this paper, we survey four (4) prominent (in terms of cybersecurity posture) NCEPs and analyze their approaches concerning incident response procedures, their cyber incidents categorization, and their roles and responsibilities in case of significant cyber incidents. Specifically, NCEPs from Germany, France, the UK, and the US are analyzed and cross-compared for the first time in literature, along with comparative data for all different NCEPs. This work provides an insight into differences and potential weaknesses of major NCEPs and proposes combinatory implementations to address documented weaknesses or risks. These data can be used by other countries or organizations to compare and update their NCEPs to remove potential weaknesses.

In Section 2 we briefly present key points in four national cybersecurity strategies, NCEPs, and their objectives and present related work in the area. In Section 3 we present each country's CI sectors and in Section 4 each country's way of categorizing cyber incidents. In Section 5 we describe the roles and responsibilities within NCEPS while in Section 6 we present the national cyber incident response procedures. Finally, in Section 7, we depict comparative data of the surveyed countries and summarize best practices, convergences, and divergences, and in Section we Discuss preliminary findings and conclude our analysis.

2. Related work

2.1 National strategies

Concerning National cybersecurity strategies and cyber emergency plans, Germany, France, the UK, and the US are four major countries that issued theoretical baselines to support cybersecurity strategies to set out their objectives. Still, only two (2) of them have formally established distinct NCEPs, in the sense of a document that precisely describes the processes in case of a significant cyber incident. This section briefly mentions the four (4) countries' national cybersecurity strategies and cyber emergency plans.

Since 2011, Germany has adopted a comprehensive cybersecurity strategy, which is frequently updated with the aim of the uninterrupted and secure operation of its CIs. The latest version of the German Cybersecurity Strategy was published in 2021 (BMI, 2021). The strategy covers the next five years and includes guidelines for the protection of organizations and a faster response to cyber incidents. In addition, it clearly describes the national goal-setting at a strategic level and focuses, among other things, on the promotion of cooperation (BMI, 2021). The country has not yet issued a distinct NCEP.

The latest French cybersecurity strategy was published in 2015 and includes five (5) strategic objectives to keep the nation cyber-secure (SSI, 2015). France has established an NCEP since 2004, known as the "Piranet Plan", which is top-secret and is only tested during exercises (Brangetto, 2015).

The UK's revised 2022 Cybersecurity Policy points to a future where the UK is even more resilient to cyber-attacks. The strategy sets out five (5) pillars to keep the UK cyber-secure (HM Government, 2022). The UK has not yet issued a distinct NCEP.

The US gives special importance to the defense of its national interests, a fact that is also reflected in the cybersecurity field, since it is one of the few countries that, in addition to its national cybersecurity strategy, has also issued a distinctive NCEP (i.e., the National Cyber Incident Response Plan - NCIPR).

The NCIRP follows five (5) basic principles to respond to incidents in the public and private sectors. (Department of Homeland Security, 2016).

2.2 Literature work

Early work on national processes concerning cyberattacks was published by Harrop and Matteson (Harrop, 2015). In their work survey potential cyber-attacks on critical national infrastructure in the United Kingdom and the USA, and discuss security measures that were drafted by these countries as mitigations controls against such threats. Albeit, important, this work does not focus on analyzing entire NCEPs, which were did not exist in their current form when this work was published. Also, authors do not critically analyze nor compare implemented approaches and lessons learned between countries, but mostly emphasize on future directions and trends in these two countries.

Work from Daricili and Cerik (Daricili, 2021) explores the relationship between the concept of national security and cyber threats, along with a theoretical analysis of cybersecurity based on the national perspective of the US. The study includes definitions of related concepts from the Turkish national cyber-defense program.

A Comparative Analysis of twenty National Cyber Security Strategies was published in 2015 (, 2015). This work aimed to use common metrics as reference to compare the cybersecurity readiness of multiple nations. Still, this work was published before the implementation of full NCEPs by major nations and mostly compares definitions, responsible authorities and types of threat characterization by each country in the study. It does not advance to more practical concepts, such as assessment process comparison, technical comparisons and implementation procedures of emergency plans (Shafqat, 2016).

3. National critical infrastructure sectors

Germany created a distinct national strategy for Cis, known as the KRITIS plan (BMI, 2021). In addition, the country created a more specialized strategy (i.e., the National Strategy for Critical Information Infrastructure Protection - CIIP Strategy) which includes structures related to IT. The competent bodies for the implementation of the aforementioned strategies are the Federal Office of Civil Protection and Disaster Assistance (BBK) and the Federal Office for Information Security (BSI) (BSI, n.d.). Germany has identified ten (10) key critical infrastructure sectors (see Table 1).

2013 marked a turning point for France's national cybersecurity strategy, as the new regulatory framework known as the CIs Information Protection (CIIP) Law was implemented. Due to the rapid increase in the number and sophistication of cyber-attacks, the country defined through the CIIP Law the critical operators, but also the obligations that these operators must fulfill. France recognized over 200 public and private critical operators from 12 CI sectors (See Table 1). (ANSSI, n.d.)

The UK has defined 13 national CI sectors (see Table 1). The responsible government body for the protection of the national CI of the UK is the Center for the Protection of National Infrastructure (CPNI). (CPNI, 2021)

The US has defined 16 CI sectors (see Table 1), the protection of which is vital for its national interests. For each sector, there is a self-governing council known as the Sector Coordinating Council (SCC) (CISA, n.d.), whose members include owners and operators of the infrastructure sectors. SCCs participate in various forums for members of all sectors to interact with each other and pursue a common policy and strategy in their efforts to ensure their resilience, including in cyberspace. (CISA, n.d.)

Table 1: Identified CI Sectors per country

Country / CI Sectors	Germany (10)	France (12)	UK (13)	USA (16)
Chemicals			X	X
Dams				X
Emergency Services			X	X
Energy	X	X	X	X
Finance	X	X	X	X
Food - Agriculture	X	X	X	X
Government - State - Administration	X	X	X	X
Health	X	X	X	X
Industry - Manufacturing - Commercial facilities		X		X
Information Technology – Communications - Broadcasting	X	X	X	X
Justice		X		
Media and Culture	X			
Military - Defence		X	X	X
Waste	X			X
Nuclear			X	X
Space		X	X	
Transport	X	X	X	X
Water	X	X	X	X

4. Cyber-incident categorization

Germany follows the BSI standard 100-4, issued in November 2008 and still in effect. In January 2021, the draft of the new standard 200-4 (BSI, 2021) was published in its 1st edition (a 2nd draft version is expected). Six (6) escalation levels are classified (see Table 2). From disaster level 6 large-scale damaging events that are not restricted to the affected entity alone to normal operation level 1 minor events. (BSI, 2009)

France follows a variant of the corresponding American scheme. Specifically, it classifies incidents into six (6) levels (level 1 is divided into 1A and 1B) (see Table 2). France takes a more "aggressive" stance in level 5 cyber incidents, which significantly differentiates it from other countries. Specifically, *these incidents are equated with "armed conflict" cases, which according to article 51 of the Charter of the United Nations, include loss of life or large-scale physical disasters*. (SGDSN, 2018)

The National Cyber Security Center (NCSC) updated UK's incident categorization system in April 2018 by increasing the categories from three (3) to six (6) (see Table 2). In this system, all incidents are included regardless of the size and role of the affected entity. A gradual involvement of agencies is noticed, during the escalation of an incident. Nonetheless, in almost all cases the response is given by the affected entity. The

exception lies in level 1 incidents, i.e., cases of national emergencies, where due to the very high severity, the response is undertaken by the government at a strategic level and the NCSC at a tactical level. (NCSC, 2018)

It is noteworthy that *level 1 and 2 incidents, combining likelihood and impact, are considered by the UK more dangerous than threats of nuclear attacks and as dangerous as international terrorism, large-scale accidents, physical disasters, and international military crises* (HM Government, 2015).

The US NCEP adopts a scheme of escalating the severity of cyber incidents. This scheme ensures that all services and agencies have a common picture of the severity of an incident to respond accordingly. According to the scheme, six (6) incident severity levels are defined, marked with different coloring (see Table 2). From level 0 (baseline - white color) which is an unsubstantiated or inconsequential event to level 5 (emergency - black color) which poses an imminent threat to the provision of wide-scale CI services, national government stability, or to the lives of U.S. persons. (The White House, n.d.) The Cybersecurity and Infrastructure Security Agency (CISA) created a national incident scoring system (National Cyber Incident Scoring System - NCISS), to rate the severity of an incident (CISA, n.d.).

Table 2: Cybersecurity Incident Severity Scale

Germany		France		UK		US	
#	**Severity level**	**#**	**Severity level**	**#**	**Severity level**	**#**	**Severity level**
6	Disaster	5	Situation of Extreme Emergency	1	National cyber emergency	5	Emergency
5	Crisis	4	Major Crisis	2	Highly significant incident	4	Severe
4	Emergency	3	Crisis	3	Significant incident	3	High
3	Early warning	2	Serious Incident	4	Substantial incident	2	Medium
2	Fault alarms	1B	Incident	5	Moderate incident	1	Low
		1A	Event				
1	Normal operation	0	Minor Event	6	Localised incident	0	Baseline

5. Roles and responsibilities

Germany follows a h*olistic approach to incident response, involving multiple agencies, entities, institutions, and even individuals*, each responsible for a part of the response process. Given that a significant incident may affect several critical sectors, the individual response per sector by different agencies is considered insufficient. Therefore, the country allocates responsibilities to the affected entities, federal agencies, and the private sector, encouraging cordial cooperation between them. To support this structure, Germany implemented a multitude of government services and agencies. It is indicative that it has staffed 57 services at the European level and 17 within the NATO framework. It has also established *67 agencies at the federal level, 34 at the state level, and 5 at the local level* (BMI, 2021) (Beigel & Herpig, 2021), the highest number in all study material.

The French National Agency for Cyber Security (ANSSI) is the official national agency for responding to cyber incidents. ANSSI belongs to the General Secretariat of the Ministry of Defense and National Security (SGDSN), an inter-ministerial body under the Prime Minister that undertakes, among other tasks, the management of national crises at a strategic level. Also, the Ministry of Defense has an active role in the country's incident response. It is noteworthy that the type of incidents reported by critical operators depends on the CI they manage. In particular, the ministry to which the respective sector of CI falls is the one that determines the type of incidents that must be reported to ANSSI. Also, this ministry assumes a coordinating role during the occurrence of incidents and defines the guidelines, objectives, contact points, vulnerabilities, and risks faced by each of its sectors, at the national level (SGDSN, n.d.).

Responsible for the UK's protection of data, networks, and CI information systems is the NCSC, which is also the cyber incident response national agency. CPNI and NCSC work closely together in the broader framework of CI security. The NCSC has an advisory role and essentially focuses on limiting the spread of a cyber incident, within the boundaries of the affected entity, to avoid a national crisis. Within the entity, if it belongs to the private sector the entity itself is solely responsible, while if it belongs to the public sector the responsibilities are distributed both to the entity and to the ministry to which it belongs. The country defends the view that "an entity that has fallen victim to a cyber-attack is also responsible for the consequences". Therefore, the NCSC is

limited to advise and analysis and only in exceptional cases deploys a response team and provides on-site support (HM Government, 2022).

In the US, the federal government has a leading role in managing the response to significant cyber incidents on entities (private or public). US NCIPR focuses on 4 lines of effort in which different federal agencies are involved. The lead federal agencies for the threat response line of effort are the Federal Bureau of Investigation (FBI) and the National Cyber Investigative Joint Task Force (NCIJTF) and they belong to the Department of Justice (DOJ). For asset response, the National Cybersecurity and Communications Integration Center (NCCIC) takes over and it belongs to the Department of Homeland Security (DHS), which also includes the US-CERT and the ICS-CERT. For intelligence support, the Cyber Threat Intelligence Integration Center (CTIIC) is the lead agency and it belongs to the Office of the Director of National Intelligence (ODNI). Finally, for the affected entity response effort, if a significant cyber incident affects a federal agency, then the agency has the lead responsibility for the response, while if a private entity is affected, then the entity has the lead responsibility for the response and the corresponding sector-specific agencies will assist the Federal Government to understand the potential impact on CIs.

6. Incident response procedure

Germany's response against significant cyber incidents is based on the resilience of the affected entities and the communication between the involved actors. Appropriate preparation and immediacy in information are the key points that will initially ensure the limitation and finally, the elimination of the crisis. For this reason, it implements a national IT Early Warning System (EWS) (Kossakowski, et al., 2006).].

The incident response steps include the implementation of an incident response plan within the entity, reporting of the incident to BSI, notification of the affected individuals, cyber incident assessment by CERT-Bund's IT-LZ, notification of other entities (potential targets) through Cyber-AZ, supporting the affected entity through CERT-Bund and MIRT, activation of the national crisis center IT-KRZ and finally requesting for external support, if needed. (BMI, 2005) (BSI, 2009) (BSI, n.d.) (BSI, n.d.)

France gives great importance to the exchange of information during cyber incidents. Critical operators send a notification form in the event of an incident, while ANSSI responds by providing suggestions or on-site support. In addition, affected entities may voluntarily exchange information with other critical operators. All information exchanges in which ANSSI participates are classified as confidential and are handled accordingly. Also, in addition to the response against the attacker, the country assumes a more active involvement within the affected entity. This implies that in the event of a significant incident if the country deems it necessary by a decision of the Prime Minister it acquires additional jurisdiction to undertake any action. It could also take control of the information systems of the affected entity, regardless of whether it belongs to the public or private sector. (ANSSI, n.d.) (Brangetto, 2015).

UK's NCSC suggests to entities the preparation of an indicative plan when a significant cyber incident takes place. To respond successfully, the entity must follow the steps below:

Step 1: Understand the type and severity of the incident.
Step 2: Kick-off Response – Reporting.
Step 3: Incident Management.
Step 4: Escalation and decision making.
Step 5: Review and close down - lessons learned. (NCSC, n.d.)

In the US, public or private entities must have cyber incident response plans in place to protect their assets and operations. In the case of a cyber incident, the affected entity must initially make every possible effort to limit the effects and secure its assets. When an incident endangers the entity's CIA, resulting in significant damage to business functions, the entity must submit a report to the corresponding federal agency, by providing basic information about the incident. The US legislation does not make reporting mandatory for the private sector, while government agencies are required to report within a specific time frame. In the event of a significant cyber incident, the Cyber Unified Coordination Group Cyber (UGC) undertakes the operational coordination of the incident response. (Department of Homeland Security, 2016)

7. Best practices – Convergences and divergences

The analysis of the NCEPs revealed significant differentiations between countries. Even within the EU, where European legislation is common to the member states, there is a certain difference in opinions and practices on important issues. Of course, there are also areas in which most member states follow the same line, for example in the selection of CIs, where no notable discrepancies are found.

7.1 Comparison of incident handling models

The models applied at a national level are mainly divided into centralized and decentralized. A centralized model applies in EU countries (i.e., France and Germany). When significant incidents occur, the competent agencies take full control of specific actions, having a correspondingly increased share of responsibility. On the other hand, in the US and the UK, the decentralized model applies. This model provides a more flexible policy with government agencies playing a more consultative role and responsibilities being shared between the involved entities.

It is worth noting that the decentralized model of the UK and the US follow a different way of diffusing the responsibility that arises from managing an incident. The risk of incident handling is often shifted to private companies or agencies that undertake the handling of an incident (perhaps entirely), without the competent agencies imposing or undertaking an active or interventional role (HM Government, 2022) (Department of Homeland Security, 2016).

In contrast, the centralized models of France and Germany take an active role in incident handling and often impose procedures and organizational security measures on the actors involved, even under the threat of fines in case they do not fully comply.

7.2 Distinct national cyber emergency plans

An important issue that was identified is that most countries have not issued a distinct NCEP to handle cybersecurity incidents and simply include instructions attached to their national strategy or in separate documents. For example, Germany has a plan for national crises (not for cyberspace) and supports many IT standards through the BSI, but no concise and comprehensive text describes the sequence of actions when significant cybersecurity incidents occur.

On the other hand, the US issued a comprehensive NCEP that clearly and accurately describes the actions of the involved entities. France also has a distinct plan, which is top-secret, while the UK is based on a set of directives, similar to Germany's.

7.3 Involved entities

Differentiations are also ascertained in the number of organizations involved when a large-scale cyber-attack takes place. For example, Germany as a federal state, involves a large number of agencies, making it difficult to determine jurisdictions and the level of involvement between these agencies. This tactic is not only a waste of resources, but it makes the system rigid, with little adaptability to the ever-changing conditions of cyberspace. In addition, the information exchange gets more difficult, since the number of recipients increases and by extension, the possibility of incorrect information or omission of an important recipient also increases.

On the contrary, France and the UK involve significantly fewer agencies. France has fully staffed the corresponding government agencies in recent years. These different approaches to the organization and structure of the country response mechanism are estimated to be mainly due to the structure of the country itself (e.g., federation), the geopolitical environment (e.g., neighboring threats that increase the possibility of cyber-attacks), and the large fluctuations of available funds and personnel.

Regarding the government and private sector relationship, some of the aforementioned countries use control mechanisms to enforce their policies, while others rely on the cooperation and initiative of the private sector. For example, Germany (less) and France (more) take a strict posture towards private companies that manage CIs. According to the law, specific or minimal measures must be taken by private companies to protect their sensitive information systems. At the same time, government agencies conduct regular audits on the implementation of these measures.

Especially France has legislated the direct involvement of state bodies in the internal systems of companies, in case of national interest reasons (Brangetto, 2015) (Cymutta, 2020). In contrast, the US and the UK apply looser legislation and invest in mutual trust and voluntary implementation of the proposed directives, hoping that the private sector will take the necessary protective measures on its own.

7.4 Involvement of military services

Another important factor worth mentioning is the involvement of the Ministry of Defense and in general the military sector of the states in dealing with cyber-attacks. For example, France actively involves the military in incidents categorized at the highest level of the country's classification scale, thus seeking to give a different dimension to incident response methods, both substantively (increased military technological capabilities) and semantically (escalating the reaction and intimidating the attacker). In case a cyber-attack was instigated by another country, France favors a more aggressive than defensive response, even with military involvement. Regarding the other countries, the military authorities are not actively involved, except in Germany, where they participate in cyber exercises for coordination and information purposes.

7.5 Incident classification

Concerning cyber incident classification, all countries distinguish six (6) basic levels of severity, with minor differences in their designation. In practice, however, no incident level is identical, nor does it escalate in the same way. Trying to fit it an incident into similar levels in different national classifications proved to be a difficult task that requires additional resources and does not necessarily capture the essence of each country's response similarities. Therefore, there is a high probability that it will lead to conclusions. On the other hand, incidents are classified mainly for practical reasons, i.e., that all involved entities "speak" the same language and that there are automated procedures and pre-defined response steps, to be able to extract statistical data for use in future threats (ENISA, 2010). To this end, we built a comparative table of the incident classification of the four (4) government entities (see Table 3) that allows for multiple cross-comparison of a specific incident against multiple national levels.

Table 3: Comparative case classification data of the surveyed countries

Case \ Country	Germany	France	UK	USA
No. of incident severity levels	6	6	6	6
Incident severity levels	1. Disaster 2. Crisis 3. Emergency 4. Early warning 5. False alarm 6. Normal functions	1. Extreme emergency 2. Big Crisis 3. Crisis 4. Significant incident 5. Event 6. Small event	1. National cyber emergency 2. Highly significant incident 3. Significant incident 4. Substantial incident 5. Moderate incident 6. Localised incident	1. Emergency 2. Severe 3. High 4. Medium 5. Low 6. Baseline
Important classification criteria	- Impact on critical assets or basic functions of the entity. - Maximum tolerable time of loss. - Expanding impact outside the entity.	- Impact on critical assets or basic functions of the entity. - Intention of the attacker. - Expanding impact outside the entity.	- Impact on critical assets or basic functions of the entity. - Expanding impact outside the entity.	- Impact on critical assets or basic functions of the entity. - Observed activity and intention of the attacker. - Expanding impact outside the entity. - Loss of human lives. - Country destabilization.

Country / Case	Germany	France	UK	USA
External support	Incident levels 1 and 2.	Incident levels 1, 2, and 3 (At level 1 the national authority acquires full access).	Incident levels 1 and 2.	Incident levels 1 and 2.
Simple Guidance	Incident levels 3, 4, and 5.	Incident levels 4, 5, and 6.	Incident levels 3, 4, 5, and 6.	Incident levels 3, 4, 5, and 6.

Preliminary results from indicative examples show that, across all countries, the highest two (2) levels (highest three (3) for France) are those that usually require external active support from the respective national body and concern situations with an impact at the national level, while the rest are most often eliminated by the affected entity with simple guidance of the national agency or other federal agency. Classification criteria remain largely similar across all NCEPs, although the quantitative scales differ, which is expected given the different size and focus on OES in these countries. **Error! Not a valid bookmark self-reference.** compares the most important criteria of the surveyed countries.

Table 4: Most important comparative criteria of the surveyed countries

Country / Criteria	Germany	France	UK	USA
Number of CIs	10	12	13	16
Model	Centralized		Decentralized	
Distinct national plan	Yes	Yes (confidential)	No	No
National response agency	BSI	ANSSI	NCSC	NCCIC, CTIIC
Role in significant incidents	Coordinator	Coordinator - Managerial	Consultant - Coordinator	
Structure - organizing	Rigid		Flexible	
Military involvement	Yes		No	
On-site support	Yes			
Measures were taken by entities	Mandatory		Optional	

8. Discussion and Conclusions

Each NCEP reflects the countries on tendencies and public sector organization. Countries, such as the UK and the US focus more on an audit-based approach while leaving enough room to organizations to build their own cyber security posture. Still, major fines and legal consequences are due in case organizations prove to be unready to major attacks, especially when these attacks impact their national citizens.

Contrary to this, Germany and France follow a more “public-sector based” approach, where the public sector and the government have an active role in managing and micro-managing the implementation of cyber-security processes and measures.

Different approaches are also found regarding the willingness of the examined states to cooperate or even request support from other states and international organizations when dealing with significant cyber incidents. For example, the UK is cautious about the possibility of cooperating with another country against a known cyberthreat, even if it is ascertained that the source of the cyber-attack is in this country (Collier, 2017). Although the UK is actively involved in international efforts to tackle cybercrime, it appears to distrust other countries to the extent of allowing them to participate in addressing a national crisis on its soil, especially after Brexit. On the contrary, countries such as Germany and France base their defense on partnerships and seek common responses both at the national and European levels.

The current perspective shows that both management models, whether government-centered (e.g. Germany) or industry-centered (UK) suffer from major issues concerning their viability against different types of cyber threats. For example, the federated approach of Germany is too slow to react in fast-paced cyber-attacks that hit multiple organizations at the same time. On the other hand, the UK’s approach to allowing organizations to tackle their own threats as they see fit, leaves room for error and negligence, especially in SMEs, while at the same time creating fertile ground for information isolation and lack of information flow in terms of coordination

and clarity. The UK and US have a mandate to inform the state of potential cyber-incidents, but history has shown that often, companies are reluctant to share information and disclose their cyber-breaches weeks or even months after they have taken place, which leaves enough time for attackers to advance and capitalize on their spoils.

It seems that a more hybrid approach, where the government plays an active role in enforcing and auditing organizations, especially OES and Cis, while at the same time allowing their leadership the responsibility required to act in time and adjust security measures and procedures to each one's way-of-work, creates the best intersection of both models.

Acknowledgements

This work has been supported in part by a Research Grand on Cybersecurity offered by the Hellenic Ministry of Digital Transformation to the Athens University of Economics and Business, Greece (2022-24).

References

ANSSI, n.d. CIIP IN FRANCE - FAQ. [Online]
Available at: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/faq/
[Accessed 09 2022].

Beigel, R. & Herpig, S., 2021. Germany's Cybersecurity Architecture. [Online]
Available at: https://www.stiftung-nv.de/sites/default/files/eng_impulse-germanys_cybersecurity_architecture_translation_of_the_6th_german_edition_0.pdf
[Accessed 09 2022].

BMI, 2005. National Plan For Information Infrastructure Protection. [Online]
Available at: https://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf
[Accessed 09 2022].

BMI, 2021. Cybersicherheitsstrategie für Deutschland 2021. [Online]
Available at: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=D8CB089E599784260FAD110D0DD36D39.1_cid373?__blob=publicationFile&v=1
[Accessed 09 2022].

Brangetto, P., 2015. National Cybersecurity Organisation: France. [Online]
Available at: https://ccdcoe.org/uploads/2018/10/CS_organisation_FRANCE_032015_0.pdf
[Accessed 09 2022].

BSI, 2009. BSI-Standard 100-4. [Online]
Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1
[Accessed 09 2022].

BSI, 2009. BSI-Standard 100-4. [Online]
Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-4_e_pdf.pdf?__blob=publicationFile&v=1
[Accessed 09 2022].

BSI, 2021. BSI-Standard 200-4. [Online]
Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD_2_0.pdf?__blob=publicationFile&v=5
[Accessed 09 2022].

BSI, n.d. Incident Response with CERT-Bund and MIRT. [Online]
Available at: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Vorfallunterstuetzung/MIRT/mirt.html
[Accessed 09 2022].

BSI, n.d. National IT Crisis Management. [Online]
Available at: https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Service-fuer-KRITIS-Betreiber/IT-Krisenreaktionszentrum/Nationales-IT-Krisenmanagement/nationales-it-krisenmanagement_node.html
[Accessed 10 2022].

BSI, n.d. What are Critical Infrastructures?. [Online]
Available at: https://www.bsi.bund.de/EN/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html
[Accessed 09 2022].

CISA, n.d. CISA National Cyber Incident Scoring System. [Online]
Available at: https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System
[Accessed 09 2022].
CISA, n.d. Critical Infrastructure Sectors. [Online]
Available at: https://www.cisa.gov/critical-infrastructure-sectors
[Accessed 09 2022].
CISA, n.d. Sector Coordinating Councils. [Online]
Available at: https://www.cisa.gov/sector-coordinating-councils
[Accessed 09 2022].
Claridge, D., 2022. Israel Bolsters Digital Defense amid Iran Cyber Threat. [Online]
Available at: https://www.geopoliticalmonitor.com/israel-bolsters-digital-defense-amid-iran-cyber-threat/
[Accessed 10 2022].
Collier, J., 2017. Strategies of cyber crisis management: Lessons from the approaches of Estonia and the United Kingdom. [Online]
Available at: https://www.politics.ox.ac.uk/sites/default/files/2022-03/strategies-of-cyber-crisis-management.pdf
[Accessed 09 2022].
CPNI, 2021. Critical National Infrastructure. [Online]
Available at: https://www.cpni.gov.uk/critical-national-infrastructure-0
[Accessed 09 2022].
Cymutta, S., 2020. CCDCOE - National Cybersecurity Organisation: GERMANY. [Online]
Available at: https://ccdcoe.org/uploads/2020/12/Country_Report_DEU.pdf
[Accessed 09 2022].
Department of Homeland Security, 2016. NATIONAL CYBER INCIDENT RESPONSE PLAN. [Online]
Available at: https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
[Accessed 09 2022].
ENISA, 2010. Good Practice Guide for Incident Management. [Online]
Available at: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
[Accessed 09 2022].
HM Government, 2015. National Security Strategy and Strategic Defence and Security Review 2015. [Online]
Available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
[Accessed 09 2022].
HM Government, 2022. National Cyber Strategy 2022. [Online]
Available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf
[Accessed 09 2022].
Kossakowski, K.-P., Sander, J., Grobauer, B. & Mehlau, J. I., 2006. CarmentiS A German Early Warning Information System-Challenges and Approaches-. [Online]
Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.123.6333&rep=rep1&type=pdf
[Accessed 09 2022].
Lohrmann, D., 2022. Cyber Attacks Against Critical Infrastructure Quietly Increase. [Online]
Available at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-attacks-against-critical-infrastructure-quietly-increase
[Accessed 10 2022].
NCSC, 2018. New Cyber Attack categorisation system to improve UK response to incidents. [Online]
Available at: https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents
[Accessed 09 2022].
NCSC, n.d. Incident management. [Online]
Available at: https://www.ncsc.gov.uk/collection/incident-management/cyber-incident-response-processes
[Accessed 09 2022].
Pearson, J. & Bing, C., 2022. The cyber war between Ukraine and Russia: An overview. [Online]
Available at: https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/
[Accessed 10 2022].
SGDSN, 2018. Revue Stratégique de Cyberdéfense. [Online]
Available at: http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf
[Accessed 09 2022].
SGDSN, n.d. SGDSN IN ENGLISH. [Online]
Available at: http://www.sgdsn.gouv.fr/accueil/sgdsn-in-english/
[Accessed 09 2022].

SSI, 2015. French National Digital Security Strategy. [Online]
Available at: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[Accessed 09 2022].

The White House, n.d. Cyber Incident Severity Schema. [Online]
Available at:
https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf
[Accessed 09 2022].

Trend-Micro, 2022. The State of Industrial Cybersecurity, s.l.: Trend-Micro.

Wayne Harrop and Ashley Matteson. Cyber resilience: A review of critical national infrastructure and cyber- security protection measures applied in the uk and usa. In Current and Emerging Trends in Cyber Operations, pages 149‑166. Springer, 2015.

Daricili, A. Burak, and Soner Celik. "National Security 2.0: The Cyber Security of Critical Infrastructure." PERCEPTIONS: Journal of International Affairs 26.2 (2021): 259-276.

Shafqat, Narmeen, and Ashraf Masood. "Comparative analysis of various national cyber security strategies." International Journal of Computer Science and Information Security 14.1 (2016): 129-136.