CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National CERT/CSIRT – Mandate and Organisation

Taťána Jančárková, Grete Toompere

NATO Cooperative Cyber Defence Centre of Excellence

About the authors

Taťána Jančárková was a researcher at the Law Branch of NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, from 2019 to 2023. Her research interests included the application of international law to cyberspace operations (Interactive Cyber Law Toolkit project), the regulatory aspects of critical information infrastructure protection, and national cyber defence frameworks. Prior to her posting at NATO CCDCOE, she had served as a legal adviser and led the International Organisations and Law Unit at the National Cyber and Information Security Agency of the Czech Republic. Ms Jančárková holds master's degrees in law and in Russian and East European studies from Charles University in Prague and an LL.M. in public international law from Leiden University.

Grete Toompere worked at CCDCOE from 2021 to 2023 as an international law researcher in the Law Branch. She was responsible for education and training in cyber law matters and was involved in cyber exercises. Her main research areas of interest were information operations and hybrid warfare. Upon completing her assignment at CCDCOE, she returned full-time as legal adviser and international cooperation officer to the Estonian Defence Forces Cyber Command. Her previous positions include the National Defence Committee of the Parliament of Estonia. Grete Toompere graduated from the University of Tartu, Faculty of Law.

CCDCOE

The NATO CCDCOE is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE comprises a diverse group of international experts drawn from military, government, academia, and industry, currently representing 39 nations.

The CCDCOE maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational, and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cyber security into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations, and law.

The Tallinn Manual, prepared at the invitation of the CCDCOE, is the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields gives cyber security experts the opportunity to enhance their skills in defending national IT-systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies, and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decision makers from the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring.

The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Acknowledgement

A heartfelt thank you of the authors goes to Anna Blechová, stagiaire at the CCDCOE Law Branch, whose editorial assistance has been invaluable to the paper.

Table of Contents

1. Abstract 5
2. Introduction 6
3. National cyber security governance 8
   - 3.1 Who is responsible for cyber security? 8
   - 3.2 National CERTs/CSIRTs as the pillars of critical information infrastructure protection 9
   - 3.3 Armed forces and the place of their incident response teams in the national cyber security governance structure 11
4. CIV/MIL cooperation in cyber security 13
   - 4.1 National cooperation 13
   - 4.2 International cooperation 15
5. Conclusions – gaps, opportunities and recommendations 17
6. References 19
7. Annex – Survey questions 21

1. Abstract

This study explores the regulatory frameworks governing the functioning of national CERT/CSIRT capabilities across NATO countries. Special focus has been given to civilian/military cooperation and the incorporation of military capabilities into national crisis management mechanisms. The conclusions are based on desk research complemented by outcomes of a questionnaire-based survey among the member states of the NATO CCDCOE. Further information has been acquired through informal interviews with national representatives during the research period. The interest of the research was in peacetime situations and cyber operations under the threshold of use of force.

The report contains three substantive sections. First, it looks in general at the cyber security governance frameworks in the target countries, identifying their main responsibilities and competent authorities, and further discusses the role of civilian and military CERT/CSIRTs in terms of their constituencies and their place in national crisis management mechanisms. The second section explores examples of civilian-military cooperation at both national and international levels. Mindful of the sensitivity, our primary aim was to determine whether such cooperation existed and, if so, then what categories of activity were covered in general. The paper presents the results as an aggregate and does not necessarily make country-specific attributions. The final section of the report seeks to formulate recommendations for better crisis management and cyber security that might stem from the parallel existence of CERT/CSIRT capabilities across national civilian and military environments.

Our research shows that all responding states have civil-military digital/cyber cooperation established at the national level, either by law or under specific agreements and arrangements, confirm that these states are not working within a cyber security vacuum and will collaborate as or when needed or required. Nevertheless, the cooperation frameworks appear to largely reflect the traditional model of the deployment of armed forces on home soil in peacetime, i.e., in a limited supportive role when dealing with large scale emergencies. That, however, often implies specific legal procedures, such as declaring a state of emergency, a state of war or other formal approval procedures ascending to the highest executive or legislative levels. Such structures of governance might prove cumbersome, if not outright counterproductive, in a cyber context.

The collaborative aspect of civilian authorities and their military counterparts indicates potential nonetheless, particularly when taking into account the limited human and financial resources states available in the context of cyber security. It is notable that many states also have international cooperation arrangements, be they bilateral or multilateral, serving as yet further confirmation of the borderless nature of cyberspace and the threats it enables to spread.

Based on the findings, a set of recommendations is made for a further strengthening of civil/military cooperation within national cyber incident response capabilities.

2. Introduction

Institutionalisation of cyber capabilities has been a well-known feature in NATO member states and other countries for decades now. With the institutionalisation comes the need for a regulatory framework, one that outlines and shapes their organisation and mandate, as well as their role in national crisis management mechanisms. Technical capabilities are commonly organised into CERT/CSIRT teams which have evolved as a standard for incident response, with set procedures and standards followed quasi-globally.[1] While the civilian CERT/CSIRT type of teams has become a regular part of national security frameworks, particularly after the European Union (EU)'s adoption of the first NIS directive in 2016, the place and role of the corresponding military capabilities in the system remain considerably less well understood. Yet, their expertise can provide an invaluable contribution to the management of large-scale crises in both peacetime and in armed conflict. Further, as human and material resources are finite, nations are bound to look into ways of using those synergies presented by incorporating their military capabilities into civilian mechanisms or by engaging civilian resources in support of national defence. The afore mentioned, however, cannot lead to compromising on the fundamental values and control mechanisms underpinning the activities of armed forces in a democratic state, adding further to the administrative and logistical challenges of those nations aspiring to reconcile the two worlds.

This study explores the regulatory frameworks governing the functioning of national CERT/CSIRT capabilities in NATO countries. Special focus has been given to civilian/military cooperation and the incorporation of military capabilities into national crisis management mechanisms.

The conclusions are based on desk research complemented by the outcomes of a questionnaire-based survey distributed among the member states of the NATO CCDCOE that are members of NATO.[2] Further information was acquired through informal interviews with national representatives during the research period. The focus of the research was on peacetime situations and cyber operations under the threshold of use of force.

In this context, it is notable that different actors and states may have different levels of understanding of the concepts of cyber security and cyber defence, as previous research has repeatedly shown.[3] The scope of this report is cyber security and/or cyber defence within the meaning of mission assurance and

---

[1] A Computer Emergency Response Team (CERT) is a group of information security experts responsible for the protection against, detection of and response to an organization's cyber security incidents. A CERT may focus on resolving incidents such as data breaches and denial-of-service attacks as well as providing alerts and incident handling guidelines. CERTs also conduct ongoing public awareness campaigns and engage in research aimed at improving security systems. Regardless of whether they are referred to as a CERT, CSIRT, CIRT or any other similar acronym, the role of all computer emergency response teams is fairly comparable. All of these organisations are trying to accomplish the same incident response related goals of responding to computer security incidents with a view to regaining control and minimising damage. To this end, they may provide or assist with effective incident response and recovery and in preventing computer security incidents from recurring. In general, an incident response team is responsible for protecting the organisation from computer, network or cyber security-related problems that may threaten an organisation and its information. A universal model for incident response, and one that has been in use for a long time, is the "protect, detect and respond" model. https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team#:~:text=A%20Computer%20Emergency%20Response%20Team,to%20an%20organization's%20cybersecurity%20incidents.

[2] See Section 2.3 for more details on the methodology used and the Annex for a copy of the questionnaire.

[3] See, e.g., Štrucl, Damjan. *Comparative Study on the Cyber Defence of NATO Member States*. Tallinn: CCDCOE Publications, 2021. https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

protection of critical infrastructure, whereas offensive capabilities and support to military operations are touched upon only marginally and where necessary.

The report contains three substantive sections. First, it looks in general at the cyber security governance frameworks in the target countries, identifying the competent authorities and their primary responsibilities, and going on to discuss the role of civilian and military CERT/CSIRTs in terms of their constituencies and their place in national crisis management mechanisms. The second section explores examples of civilian-military cooperation at both national and international levels. Mindful of the sensitivity, our aim was primarily to determine whether there was any such cooperation and, where such cooperation was identified, what general categories of activity were covered. The paper presents the results as an aggregate and does not necessarily seek to make country-specific attributions. The final section of the report seeks to formulate recommendations for better crisis management and cyber security that might stem from the parallel existence of CERT/CSIRT capabilities across national civilian and military environments.

3. National cyber security governance

3.1 Who is responsible for cyber security?

The need to protect critical information infrastructure and establish corresponding national capabilities has been stressed by both NATO and the EU for many years. While "cyber security" [4] and "cyber incident" [5] are NATO-agreed terms, so as far as critical infrastructure and critical information infrastructure are concerned, there is no such equivalent NATO definition.[6] The term and its content have thus remained within the remit of individual nations.

For 22 of 31 NATO member states who are also EU members, the situation was clarified in 2016 with the adoption of the Directive on Network and Information Systems Security (the so-called NIS directive).[7] Despite avoiding the terms 'critical infrastructure' and 'critical information infrastructure', the directive provided a baseline list of sectors and services that were to be protected, outlined the functions a state should guarantee and the structures it should put in place in order to ensure such protection. The directive's 2022 revision took the governance and the capabilities-related obligations further to cover yet more services and entities, as well as to endow the competent authorities with greater powers of supervision and enforcement.[8]

Among other aspects, the NIS directive has obliged countries to establish at least one competent authority and at a minimum one CSIRT-type team to cover the regulated services. The directive did not however prescribe a specific governance model. Even those EU countries which had, until then, lingered in building their national cyber security governance structures have now had to comply with the NIS directive. EU candidate countries have since also sought to align their legislative and institutional frameworks. Among these applicants, three are currently NATO members, specifically Albania, Montenegro, and North Macedonia.

The national models chosen vary, reflecting respective constitutional configurations and administrative traditions. Thus some countries have opted for a more centralised approach and have one competent authority and one CERT/CSIRT catering to the sectors identified in the NIS directive, including the government and public administration, [9] whereas others have chosen a sectoral approach and have designated a competent authority and CERT/CSIRT for individual sectors or their groups, or even for

---

[4] Application of security measures for the protection of communication, information and other electronic systems, as well as the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation. https://nso.nato.int/natoterm/Web.mvc

[5] Any detected anomaly compromising or that has the potential to compromise communication, information or other electronic systems or the information that is stored, processed or transmitted in these systems. https://nso.nato.int/natoterm/Web.mvc

[6] Starting from the NATOTerm, the official NATO terminology database, through other NATO sources, including AJP-3.20, the Allied Joint Doctrine for Cyberspace Operations, critical infrastructure is always mentioned as something essential and worth protecting, yet no official definition for NATO can be found.

[7] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016.

[8] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyber security across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), OJ L 333, 27.12.2022.

[9] France (see https://www.cert.ssi.gouv.fr/a-propos/) or the Czech Republic (see Section 20 of the law 181/2014 Coll., on Cyber Security, available at https://www.nukib.cz/en/cyber-security/regulation-and-audit/legislation/).

infrastructure within the territorial administrative unit of a country.[10] There are also countries where one national CERT/CSIRT is responsible for the essential services under the NIS directive while another caters to public administration/government infrastructure.[11]

The remaining 6 NATO and non-EU member states, specifically Canada, Iceland, Norway, Türkiye, UK, and the USA, have also adopted measures to develop incident response capabilities. There is also a visible trend of moving away from voluntary compliance-based systems of security measures and incident reporting towards mandatory ones.[12]

In any event, every NATO member state today possesses a cyber/computer incident response capability covering (or otherwise working towards covering) the country's most critical economic and societal sectors. The scope of regulation is laid down in legislation[13] and, in some instances, stated within strategic policy documents of national significance. All states also have an entity, whether this be a ministry or a designated agency tasked with CII protection, risk management planning, incident response, or other responsibilities related to cyber security.

3.2 National CERTs/CSIRTs as the pillars of critical information infrastructure protection

As outlined in Section 3.1, it has become a standard practice among NATO states to have, or else to be developing, at least one national level incident response team of the CERT/CSIRT-type that typically caters for those critical or essential services dependent on information and communication technologies. All EU member states have transposed the NIS directive obliging them to have such capability, and belong to a Union-wide cooperation network of CSIRT teams.[14] Additionally, most countries aspiring to EU membership, and several of those that have signed an association agreement with the EU, have either implemented or plan to implement the NIS directive to some extent, or at least have or are in the process of establishing a national CSIRT/CERT.[15] Non-EU NATO countries have also established a

---

[10] Germany (see https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/Nationale-und-internationale-Zusammenarbeit/nationale-und-internationale-zusammenarbeit_node.html), Slovakia (see Section 9 in conjunction with Annex 1 of the law 69/2018 Coll., on Cybersecurity and on Amendments and Supplements to Certain Acts, available at https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf).

[11] Slovenia, for instance (see Section 1 of law 2018-01-1350, on Information Security, available at https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2018-01-1350?sop=2018-01-1350).

[12] See Canada's draft Bill C-26, available at https://www.parl.ca/legisinfo/en/bill/44-1/c-26, the US National Cybersecurity Strategy issued on 2 March 2023, available at https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf or the US Cyber Incident Reporting for Critical Infrastructure Act of 2022, available at https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-o-f2022_508.pdf.

[13] In most cases, relevant legislation has been adopted and is in force, although there are a few instances of NATO countries that are only working to prepare the necessary legislative instruments.

[14] See https://csirtsnetwork.eu/ for more information.

[15] Cf. Art 1(2) of the Kosovo Act on Cybersecurity, available at https://www.kuvendikosoves.org/Uploads/Data/Documents/Ligjinr.08-L-173_Lt5nfFXujr.pdf; National Cyber Security Strategy of the Republic of North Macedonia and the information on transposition of the NIS directive available at https://mioa.gov.mk/sites/default/files/pbl_files/news/transponiranje-na-direktivata-1148-2016-za-obezbeduvanje-na-visoko-nivo-na-bezbednost-za-mrezi-i-informaciski-sistemi-1271.nspx, https://mioa.gov.mk/mk-MK/news/nacionalna-strategija-i-akciski-plan-za-sajber-bezbednost-na-republika-severna-makedonija-2018-2022-1813.nspx; or the assessment of the draft information security law of Georgia, criticised for a lack of compliance with the NIS directive: https://idfi.ge/public/upload/GG/CyberN333.pdf. All these

CERT/CSIRT capability at the national level.[16] Compared to a decade ago, it can be said that CSIRT/CERT has become a common occurrence.

Three elements define a CERT/CSIRT and need to be addressed when such a capability is being considered.[17]

First, the mission of the CERT/CSIRT. This should be identified, stated in the security team's founding documents and publicly accessible. Websites of individual CERT/CSIRT teams refer to a safeguarding function and response to cyber attacks; the detection of vulnerabilities or protection against incidents;[18] the analysis of cyber threats and vulnerabilities; the dissemination of cyber threat warning information and coordination of incident response activities;[19] and, the management of security incidents within their respective national domains.[20] In general, the mission entails prevention, information, coordination, and incident management. The mission also defines the actual services a CERT/CSIRT team provides, depending *inter alia* on the team's maturity and resources.

Second, what will be the constituency? National CERT/CSIRT teams that are the subjects of this study cater, by default, to the most important and vital services which underpin the nation's societal and economic well-being. As mentioned above, some CERT/CSIRTs cover the full spectrum of such services, while others only address selected sectors.

The third element, and possibly the most interesting in the context of this study, is the institutional anchoring of the CERT/CSIRT. The efficient and effective fulfilment of its mission requires that a national CERT/CSIRT be part of the national security community and be able to coordinate and exchange information with stakeholders relevant to its work across the government and society.

In the early phases of the development of national cyber security governance, CERT/CSIRT teams and the cyber security portfolio, as such, were typically to be found within the ministry of defence or the ministry of the interior. Several NATO/EU countries had established their cyber security authority and CERT/CSIRT function with an intelligence service which previously held responsibility for signal intelligence and communications protection.[21]

With the advent of the NIS Directive and a generally increased awareness of the importance of cyber security in the protection of a nation's critical infrastructure, a shift in favour of establishing specialised

---

countries, however, have a national CERT/CSIRT team. The same applies to Türkiye (https://www.first.org/members/teams/tr-cert) or Ukraine (https://www.eeas.europa.eu/eeas/ukraine-and-eu-held-second-round-ua-eu-cybersecurity-dialogue_en).

[16] See the United States CERT or Norwegian CERT (https://nsm.no/areas-of-expertise/cyber-security/norwegian-national-cyber-security-centre-ncsc/).

[17] West-Brown, Moira, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs),* 2nd ed., Software Engineering Institute: 2003, available at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305. See also Bronk, Henk, Marco Thorbruegge, Mehis Hakkaja. *A Basic Collection of Good Practices for Running a CSIRT*. ENISA 2007, available at https://www.enisa.europa.eu/publications/a-collection-of-good-practice-for-cert-quality-assurance.

[18] CERT-FR, https://www.cert.ssi.gouv.fr/a-propos/

[19] US-CERT, https://www.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf

[20] CERT EE, https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee/monitoring-cyberspace-and-impeding-incidents

[21] The British National Cyber Security Centre that has evolved from and within the General Communications Headquarters (GCHQ) serves as an example. Denmark's Centre for Cyber Security attached to the Danish Defence Intelligence Service (DDIS) is another one.

agencies for cyber security can be discerned, be they stand-alone agencies or entities attached to a larger organisation.[22]

The widespread reach of cyber security regulation has not included the defence sector, however. The information systems and networks used by armed forces and defence ministries in managing national defence or supporting military operations have largely remained outside of their remit.[23] Their incident response teams and cyber defence capabilities have, nevertheless, a shared interest in preventing, detecting and handling cyber incidents, as well as the prerequisite skill set. So, how do they potentially fit into the national cyber security framework?

3.3 Armed forces and the place of their incident response teams in the national cyber security governance structure

Force is traditionally considered the *ultima ratio*. Armed forces members serve primarily to defend a country's territorial integrity in times of danger and their training and mandate corresponds to this purpose. The use of military personnel during peacetime is, therefore, rather limited. Outside the state of martial law, the military is used for support and assistance, although always within the remits of a specific request and related mandate. In light of historical experience, democratic countries have enshrined multiple checks and balances in their constitutional laws to prevent the military from taking over power in peacetime and to ensure civilian control over the armed forces. The deployment, or even the temporary presence of both national and foreign armed forces on the territory of a state, is subject to authorisations by the executive and often by the national legislature.

However, armed forces and military networks increasingly face the same or similar challenges as the civilian sphere and are thus not immune to malicious behaviour in cyberspace. As the military and intelligence networks are usually beyond the scope of cyber security legislation and thereby explicitly excluded from the NIS directives, an important part of our research was to find out more about the mandate of military incident response teams and whether they can intervene in national cyber crisis management and, if so, under what conditions.

All surveyed states have a CERT/CSIRTs capability responsible for military networks. Such units do not necessarily engage in support of military operations or otherwise develop offensive capabilities; indeed, they can even be administratively separated and exist under different entities.[24]

By default, it is not within the remit of the military CERT/CSIRTs to participate in the protection of the national critical information infrastructure. There are, however, exceptions to the principle, such as in the United States, where the Cyber Command is entitled to engage on domestic soil, in activities not

[22] See the Czech National Cyber and Information Security Agency (NÚKIB), established in 2017, or Italia's Cyber Security Agency, set up in 2022. The US CISA has also acquired additional competencies since its foundation in 2018. France's ANSSI is, to a large extent, also an independent agency.

[23] Within the EU, by virtue of the competencies shared among the EU and the member states, defence issues are the direct responsibility of the states and a matter of cooperation or coordination, rather than harmonisation. Cf. further Art. 1(6) of the NIS directive which explicitly excludes matters pertaining to national security from the scope of directives.

[24] Cf. Czech Republic's Communication and Information Systems Agency (AKIS), the Cyber and Information Operations Command and the National Cyber Operations Centre, are all affiliated to different entities within the Czech armed forces and the Ministry of Defence. A contrary example can be found in Poland where the Cyber Command (Dowodztwo Komponentu Wojsk Obrony Cyberprzestrzeni) includes both the CSIRT MON and the active cyber operations capabilities, along with other functions (https://www.cyber.mil.pl/ncbc-dkwoc/).

only of monitoring character (and not only within the Department of Defense's networks), or in Poland where the mandate of the Polish Cyber Defence Forces is also rather comprehensive.[25]

Our approach was first to understand the general use of national military capabilities during peacetime and, subsequently, whether the same rules and requirements would apply to military cyber units, and how those units would be used in a cyber crisis.

Our survey [26] has confirmed that NATO states have procedures in place to enable the use of the armed forces in national crisis management. Traditionally, armed forces have been used to help during natural disasters, health crises (e.g., during the COVID-19 pandemic), or in the interest of reinstating public order.

We have not found specific provisions for the military's involvement in cyber crisis management. Indeed, it is difficult to envisage such specific provisions within laws that sometimes are of a constitutional level and/or had been drafted long before states began engaging in cyberspace activities in a conscientious and consistent manner. These laws often require a high-quorum voting procedure necessitating consensus across the national political spectrum and the "opening" of constitutional legislation to accommodate cyberspace-related considerations might effectively mean opening the proverbial Pandora's box. Nevertheless, it does not mean there are no mechanisms in place to engage a military cyber capability to assist in civilian cyber crisis management.[27]

One of the survey questions was aimed at incident response mechanisms and thresholds for military involvement at both national and international levels. Five responses out of eleven confirmed the existence of a national level military involvement threshold, while two indicated another, as yet unspecified, approach with respect to overall crisis management and the division of responsibility. The remaining responders did not provide a specific answer. Complementary desk research suggests that the engagement of armed forces in such cases would be governed by the general legislation pertaining to national crisis management.

Some respondents used the opportunity to elaborate on the topic and predominantly referred to an armed attack and the state of war as the primary threshold for military involvement. Some also stated that the issue of threshold would be resolved on a case-by-case basis, with involvement increasing if a certain impact level was reached. One country explained that the impact level was usually evaluated based on the number of users affected by the incident, its effect on infrastructure and geography, its duration, and broader consequences for the national economy and society, largely reflecting the language of the NIS directive. In case of a state of war or armed attack, the military component would assume managing authority over cyber incident responders.

Regarding engagement at the international level, four countries answered in the affirmative that a formal or informal threshold existed for their military to become involved, while another seven asserted that no such threshold had been defined. Joint national authority for such an incident response was confirmed on four occasions, while six responded in the negative and one left the question unanswered.

---

[25] See https://www.cybercom.mil/About/Mission-and-Vision/ or https://www.cyber.mil.pl/ncbc-dkwoc/.

[26] We contacted all 30 NATO member states through the CCDCOE steering committee representatives. We received responses from 11 states. In addition, we received informal feedback from 11 national representatives from the ranks of CCDCOE staff seconded by NATO countries.

[27] Niall O'Connor. *A year on: Inside the Defence Forces response against the HSE ransomware hack*. The Journal, 22 May 2022, available at https://www.thejournal.ie/irish-defence-forces-cyber-security-response-5769175-May2022/.

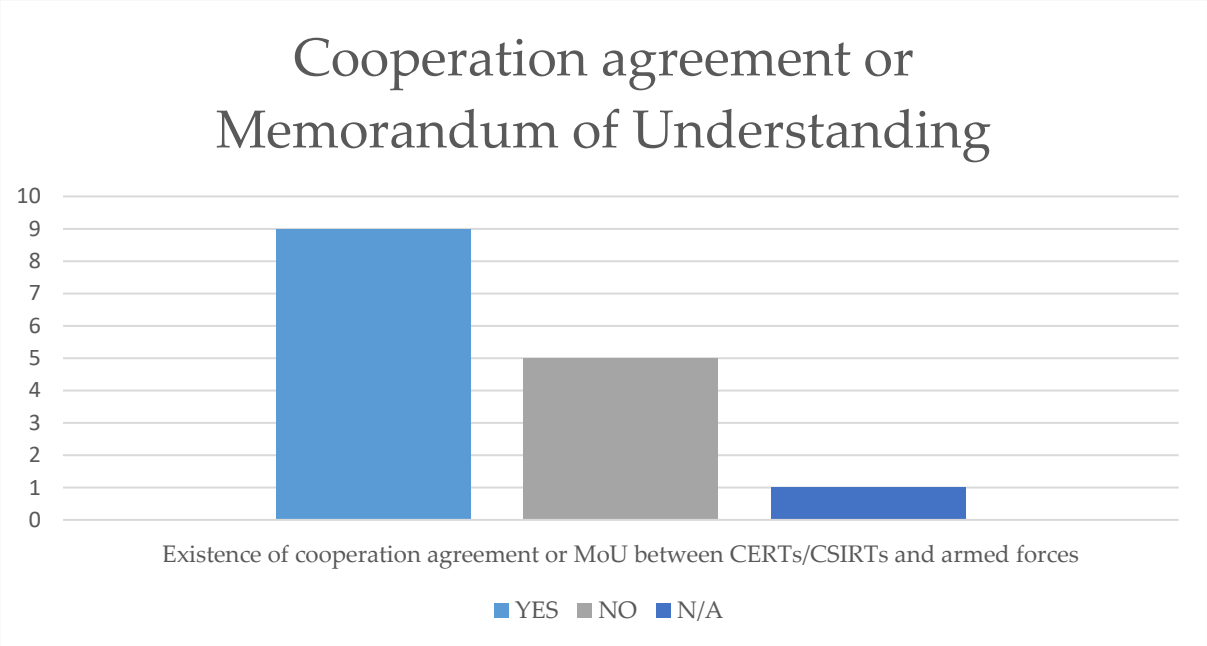
4. CIV/MIL cooperation in cyber security

The above does not imply, however, that no cooperation or coordination exists between civilian and military capabilities within national cyber security governance. Some level of regular interaction between the civilian and military components in cyber security does exist in most, if not all NATO countries. Several have reported the existence of agreements or memoranda of understanding covering various areas of activity, while others asserted working level cooperation on an ad hoc basis.

4.1 National cooperation

To complement the desk research, we first asked national representatives at the CCDCOE and then, via the Centre's Steering Committee, CCDCOE member nations for more detailed information on actual cooperation between civilian critical infrastructure defenders and their respective military counterparts. We did not inquire about the procedural specifics of incident handling or any specific details of collaboration. The results obtained through surveys that could not be corroborated by public sources are presented without attribution to a specific country.

First, we were interested in whether there was a formal cooperative agreement or a memorandum of understanding (MoU) between the national CERTs/CSIRTs and respective teams in the armed forces.



Six of the eleven responding states [28] confirmed the existence of such an instrument as a basis for collaboration. The remaining five, however, stated that such obligation derived from the law. At least one country confirmed that a formal cooperation mechanism existed, although its scope and contents were classified. Several responders added that actual cooperation extended beyond what the entities

[28] Taking into consideration the informal responses, the total number of existing cooperation arrangements was 9 out of 15.

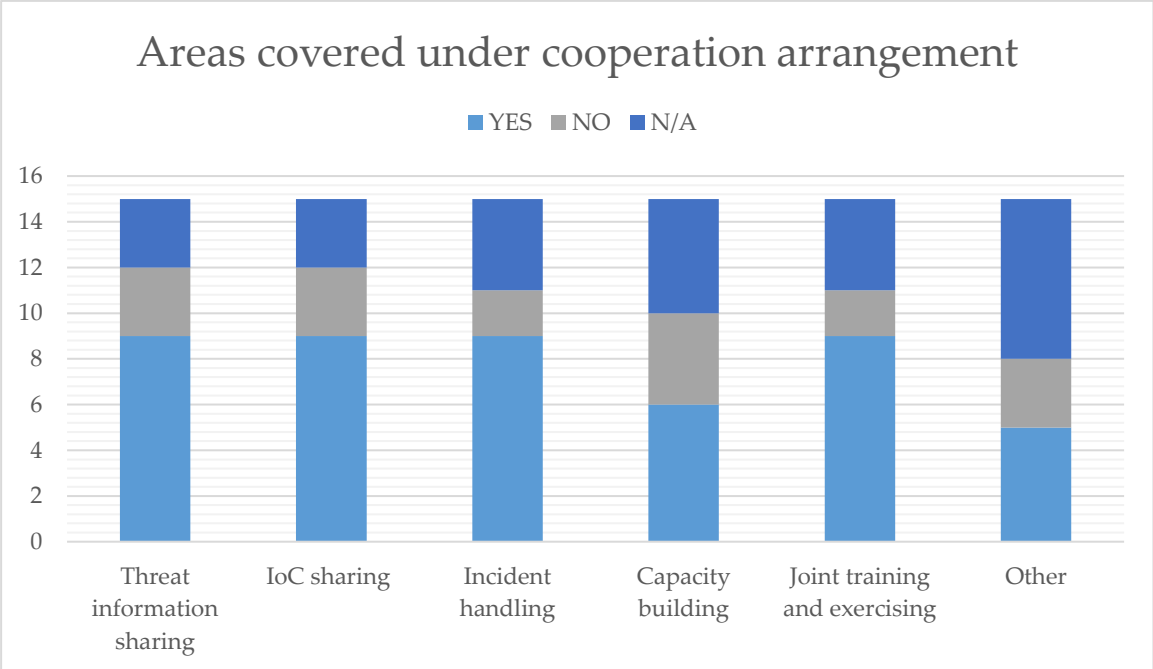
have agreed formally and most communication between those teams happens on an ad hoc basis at the working level.

Multiple states have a joint coordination capability, gathering various civilian and military stakeholders in cyber security, sometimes including even private sector representatives.[29] One state has a joint operations centre that caters for both civilian and military infrastructure.

The second question was multiple choice and sought to identify those areas covered under the cooperation arrangement. We offered the following options:

1) cyber threat information sharing,
2) indicators of compromise sharing,
3) incident handling,
4) capacity building, and,
5) joint training and exercises.

We also offered the option to add supplementary information and any other relevant details. According to the responses, the cooperation mostly covers the sharing of threat information and IoC in alignment with joint training and exercises. In several instances, cooperation also extended to capacity building and incident handling. A few responders provided additional information to the effect that their arrangements included operational-level cooperation to improve the speed of response (and the latter's quality overall), mutual and reciprocal training and internships, incident management and vulnerabilities, HR, communication and international relationships, cyber security legislation, and/or relationships with national sectoral authorities.



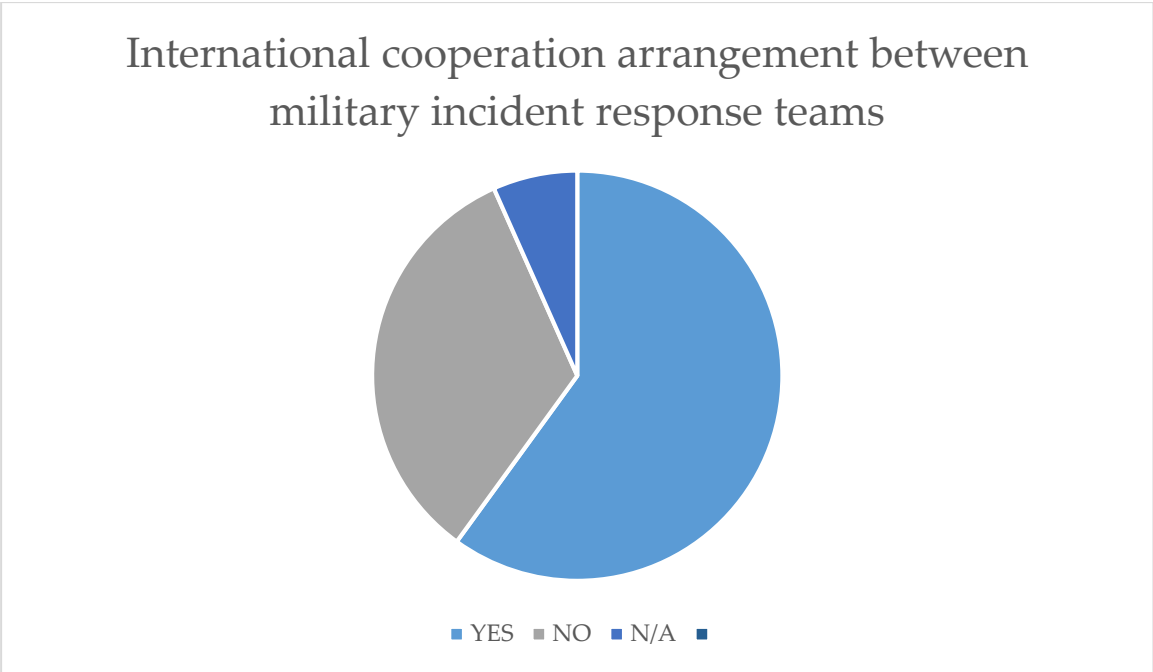
[29] See, for instance, Norway's National Cyber Security Centre and Joint Cyber Coordination Centre or Germany's National IT Situation Centre.

4.2 International cooperation

Further, we were interested to determine whether bilateral or multilateral cooperation agreements or regional arrangements had been concluded between military CERT/CSIRT and their respective counterparts in other countries. Eight respondents answered yes, while others elaborated that they had MoUs with specific countries, or were part of the PESCO Cyber Rapid Response Teams and Mutual Assistance in Cyber Security project.[30] The additional cooperation focused on cyber threat information sharing, IoC sharing, capacity building, joint training and exercises, incident handling cooperation, and sharing of national policies.

Some mentioned that their cooperation aimed at mutual assistance, vulnerability assessments and the creation of joint capabilities. Additionally, such cooperation covered information and experience sharing related to incident handling, workflows and problem management, used standards, methodologies, and best practices.

Several responders answered that there were different cooperation agreements between neighbouring countries and various international frameworks.[31]



Joint capacity building and joint training and exercises appear not to be common at the bilateral level. Nevertheless, several multilateral platforms and frameworks compensate, at least partially, for the lack of such arrangements.

Among the most recent examples, the EU has committed, in its 2022 Cyber Defence Policy, to furthering international cooperation, in particular through establishing an operational network for military CERTs/CSIRTs. All member states are called to participate in the MICNET to enhance coordination with

[30] https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/; See also https://kam.lt/wp-content/uploads/2022/03/CRRT-2018.pdf.
[31] Ironically, one country provided information on a MoU with another country. The latter, however, in their own response, denied the existence of any formal international cooperation arrangements.

civilian communities.[32] The initiative focuses on strengthening situational awareness as well as enhancing cooperation through various projects and exercises.

The EU and NATO have developed a stable and solid partnership over the years and are seeking even closer cooperation between their respective agencies, mainly through reciprocal information sharing and training. The Malware Information Sharing Platform (MISP), operated by NATO, caters for both military and civilian members. The NATO Virtual Cyber Incident Support Capability, currently under development, could, at least to an extent, provide another platform for cooperation between military incident response teams.

Further, Locked Shields and other exercises organised by the CCDCOE, regional platforms or NATO, provide an opportunity not only to train and exercise, but also to meet and network with peers.

[32] European Commission and High Representative of the Union on Foreign Affairs and Security Policy. *Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence*. JOIN(2022) 49 final. Brussels: 10 November 2022.

5. Conclusions – gaps, opportunities and recommendations

Having a dedicated team responsible for incident prevention and response safeguarding the information infrastructure that underlies those services which are deemed essential for the societal and economic functioning of a nation has become a standard in all NATO countries. While there is no common definition of critical information infrastructure at the NATO level, or at the EU level for that matter, there is a shared understanding of the need for a streamlined and coordinated approach to protect such infrastructure. The adoption of related EU-wide legislation in the past few years has sped up the efforts of states in that regard.

Armed forces, which increasingly rely on information and communication technologies in their internal processes, as well as to fulfil their primary defensive purpose, are not immune to threats from cyberspace and accordingly build their own incident response capabilities.

When it comes to interaction between the civilian and military capabilities, however, the situation is more complex, and nations seem to maintain the traditional dichotomy of functions and responsibilities between the civilian administration and armed forces. Furthermore, it appears that international cooperation between military incident response teams is not as advanced as has been the case with civilian teams. At present, there are no professional platforms such as FIRST[33] or TF-CSIRT[34] aimed at military CERTs/CSIRTs.

Nevertheless, militaries cannot run their systems and defend their information infrastructure in a perfect vacuum and a silo approach can be effective, and justified, in specific cases only. The civilian and military sectors are increasingly interdependent since the functionality of civilian infrastructure is often the prerequisite for the functioning of military infrastructure. Armed forces are dependent on the electricity grid, internet providers or transportation infrastructure. Many manufacturers supply their technologies to both the military and civilian sectors, and the latter use the same or similar tools in their incident response work. Cyber threats themselves, as well as the malicious actors, are usually not exclusively of civilian or military nature and therefore not clearly distinguishable.

The collaborative aspect of civilian authorities and their military counterparts thus acquires a potential, particularly when taking into account the limited human and financial resources states have available for cyber security.

This paper has attempted to shed a little more light on the present situation and identify the regulatory frameworks currently governing cooperation between civilian and military capabilities while identifying those areas in which cooperation takes place more commonly or has the biggest potential. The lower response rate to our survey, sent to NATO member states, naturally limits the informative value of the findings. Nevertheless, basic trends can be discerned.

Our survey has shown that all responding states have civil-military digital/cyber cooperation established at the national level, either by law or under specific agreements and arrangements, thereby confirming that these states are not working in a cyber security vacuum and will tend to collaborate when needed or required. Nevertheless, the cooperation frameworks appear to largely reflect the traditional model of deployment of armed forces on home soil during peacetime, i.e., a limited supportive role when dealing with emergencies. This, however, often implies specific legal procedures, such as declaring a state of emergency or a state of war, or formal approval procedures ascending to the highest executive or

[33] https://first.org.
[34] https://tf-csirt.org.

legislative levels. However, such a chain of command might prove cumbersome, if not outright counterproductive, in a fast-moving cyber context.

The primary areas covered by these types of cooperation agreements are information sharing related to incident information, indicators of compromise, and cyber threat intelligence. Other areas, such as joint exercises and capacity building, appear to be limited. Further, much of the cooperation takes place at the working level on an ad hoc basis, a pattern which may not ensure the required sustainability.

It is noteworthy that many states also have international cooperation arrangements, be they bilateral or multilateral, which is yet another confirmation of the borderless nature of cyberspace and the threats that come within.

Based on the above findings, the following recommendations are made:

1) Enhance reciprocal knowledge exchange opportunities and capacity building, including staff internships. In addition to sharing experience, this would help understand the tools and procedures that are used for network defence and incident response by respective institutions, as they may vary between civilian and military infrastructure.

2) Develop and implement procedures allowing for the timely and actionable exchange of information between the civilian and military structures for large scale incidents. To guarantee reciprocal functionality, it is essential that respective teams at least work together when there is an incident and, depending on the scale of the incident and whether it occurs within civilian or military infrastructure, a common solution with the best tools and equipment is of the utmost necessity.

3) If thresholds for the engagement of the military are not formally defined, they should at least be addressed internally and respective SOPs must be developed. Explore the possibilities of establishing joint coordination centres at the national level, incorporating elements from armed forces, civilian cyber security authorities but also law enforcement and intelligence services.

4) Seek joint training and exercises. If people do not have a proper opportunity to practice together during peacetime, defending during armed conflict becomes more challenging. Exercising the transition between peacetime and emergency states, including from the perspective of internal division of competencies would be of particular relevance.

5) Develop international coordination and cooperation formats for military CERTs/CSIRTs and explore opportunities for their interaction with relevant civilian platforms.

6. References

Agence nationale de la sécurité des systèmes d'information. *À propos du CERT-FR*. https://www.cert.ssi.gouv.fr/a-propos/

Bundesamt für Sicherheit in der Informationstechnik. *National and International Collaboration*. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/Nationale-und-internationale-Zusammenarbeit/nationale-und-internationale-zusammenarbeit_node.html

Bronk, Henk, Marco Thorbruegge, Mehis Hakkaja. *A Basic Collection of Good Practices for Running a CSIRT*. ENISA 2007, available at https://www.enisa.europa.eu/publications/a-collection-of-good-practice-for-cert-quality-assurance.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cyber security across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), OJ L 333, 27.12.2022.

European Commission and High Representative of the Union on Foreign Affairs and Security Policy. *Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence*. JOIN(2022) 49 final. Brussels: 10 November 2022.

Kosovo Assembly. 2023. *Law nr.08/L-173, on Cyber Security*. https://www.kuvendikosoves.org/Uploads/Data/Documents/Ligjinr.08-L-173_Lt5nfFXujr.pdf.

Malvenishvili, Mari, Nini Balarjishvili. 2022. Cybersecurity Reform in Georgia: Existing Challenges, International Practice and Recommendations. https://idfi.ge/public/upload/GG/CyberN333.pdf.

Ministry of Information Society and Administration of the Republic of North Macedonia. https://mioa.gov.mk/sites/default/files/pbl_files/news/transponiranje-na-direktivata-1148-2016-za-obezbeduvanje-na-visoko-nivo-na-bezbednost-za-mrezi-i-informaciski-sistemi-1271.nspx.

Ministry of National Defence of the Republic of Lithuania, *Cyber Rapid Response Teams and Mutual Assistance in Cyber Security. Memo for Mutual Assistance in Cyber Security, Key Roles and Procedures for the CRRTs' Operations, Lessons Learnt from the Cyber Shield/ Amber Mist 2018 Exercise.* https://kam.lt/wp-content/uploads/2022/03/CRRT-2018.pdf.

O'Connor, Niall. 2022. *A year on: Inside the Defence Forces response against the HSE ransomware hack*. 22 May. https://www.thejournal.ie/irish-defence-forces-cyber-security-response-5769175-May2022/

Parliament of Canada. *Bill C-26. An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*. https://www.parl.ca/legisinfo/en/bill/44-1/c-26.

Parliament of the Czech Republic. *Law no. 181/2014 Coll., on Cyber Security*. https://www.nukib.cz/en/cyber-security/regulation-and-audit/legislation/.

Parliament of the Slovak Republic. *Law 69/2018 Coll., on Cybersecurity and on Amendments and Supplements to Certain Acts.* https://www.sk-cert.sk/wp-content/uploads/2018/03/2018_69-Act-on-Cybersecurity.pdf.

Parliament of Slovenia. *Law 2018-01-1350, on Information Security*. https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2018-01-1350?sop=2018-01-1350.

Permanent Structured Cooperation. *Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT)*. https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/.

Polish Armed Forces. *Cyberspace Defence Forces Command*. 2022. https://www.cyber.mil.pl/ncbc-dkwoc/.

Sullivan, Peter. *What is a CERT?* https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team#:~:text=A%20Computer%20Emergency%20Response%20Team,to%20an%20organization's%20cybersecurity%20incidents.

Štrucl, Damjan. *Comparative Study on the Cyber Defence of NATO Member States*. Tallinn: CCDCOE Publications, 2021. https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf.

West-Brown, Moira, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek. *Handbook for Computer Security Incident Response Teams (CSIRTs),* 2nd ed., Software Engineering Institute: 2003, available at https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305.

US Cyber Command. 2022. https://www.cybercom.mil/About/Mission-and-Vision/.

US Congress. 2022. *Cyber Incident Reporting for Critical Infrastructure Act*. https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-o-f2022_508.pdf.

US Government. 2023. *National Cybersecurity Strategy*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

7. Annex – Survey questions

1. Does your nation have a cooperation agreement or MoU concluded between national CERTs/CSIRTs and respective teams in armed forces (including intelligence components if applicable)?..... YES/NO

Comment (optional, elaborate as appropriate)

2. What kind of topics are covered under the arrangement?

- threat information sharing……..... YES/NO
- IoC sharing……..…… YES/NO
- incident handling……..….. YES/NO
- capacity building…….……YES/NO
- joint training and exercises…….……..YES/NO
- other…….…….....YES/NO (please specify if applicable)

3. Do you have a threshold for involvement of the military in incident response by civilian CERTs/CSIRTs (and vice-versa) nationally? ……..YES/NO

And internationally? .....YES/NO

Is there a joint authority in such a situation? ……..YES/NO

Are the thresholds formally defined?…….……..YES/NO (elaborate as appropriate)

If YES and appropriate, please specify the origin of threshold definition (established formally, agreed bilaterally, defined internally, else)

4. Does your military CERT/CSIRT have bilateral or multilateral cooperation agreements or regional arrangements with respective teams in other countries? ……YES/NO

If YES and appropriate, please elaborate on the scope of cooperation.