June 2023 · Julia Schuetze and Eglė Daukšienė

Cybersecurity Support Deployments:

An emerging cooperative approach

Stiftung Neue Verantwortung

Think Tank at the Intersection of Technology and Society

Acknowledgment

This analysis was supported by the Transatlantic Cyber Forum "International Deployment of Governmental Incident Response Teams" and practitioners through online collaboration, researcher and practitioner interviews, and a joint virtual workshop.

The views and opinions expressed in this paper are those of the authors and do not necessarily reflect the official policy or position of the working group members or that of their respective employer(s).

The following individuals are acknowledged in alphabetical order for their essential contributions:

1. Richard J. Harknett, PhD, Professor & Director, School of Public and International Affairs (SPIA), Co-Director, Ohio Cyber Range Institute (OCRI)
2. Sven Herpig, Stiftung Neue Verantwortung e.V.
3. Louise Marie Hurel, Dept. Media and Communication London School of Economics and Political Science (LSE) and Royal United Services Institute
4. Koichiro Komiyama, JPCERT/CC
5. Andreas Kuehn, Observer Research Foundation America
6. Joanna Kulesza, University of Lodz / Lodz Cyber Hub
7. Rolf Lion, CERTBw, German Armed Forces
8. Christoph Lobmeyer, Incident Response Expert
9. Igor Mikolic-Torreira, CSET, Georgetown University
10. Christine Runnegar, Internet Society
11. Janine Schmoldt, University of Erfurt
12. Thomas Schreck, University of Applied Sciences Munich
13. Lina Siebenhaar, Project Cyber Command, Swiss Armed Forces
14. Leonie Maria Tanczer, University College London

Executive Summary

Purpose of this report

Governments worldwide are increasingly acknowledging the necessity of collaborative and partnered approaches to enhance cybersecurity. The scarcity of cybersecurity professionals and the dispersion of information among stakeholders in the government and the private sector have amplified the need for cooperation between governments and non-government entities. Various forms of cooperation have emerged, including information-sharing agreements, the exchange of liaison officers, and the establishment of task forces. In this context, **this paper explores a particular form of cooperation that can be considered a type of "deployment".** Originally a military term, deployment refers to "the movement of troops or equipment to a place or position for military action." **Although governments have increasingly turned to this approach in recent years, it remains a relatively understudied method of collaboration, and its characteristics and dynamics have analytically hardly been understood.** To analyze this tool in the field of cybersecurity, the working definition of "cybersecurity support deployment" in this paper is as follows: "Military and/or civilian cybersecurity support deployment can be applied when cybersecurity professionals from one country provide support to another based on their government's decision involving a cybersecurity-related activity or resources, such as hardware and software."

Requesting support from other countries for matters of national security and inviting their experts can be sensitive issues for governments. This form of support has therefore been discussed, developed, and applied by practitioners, and its implementation mostly occurred behind the scenes, away from public scrutiny. However, insufficient knowledge and misunderstandings of the concept of deployment missions in public can lead to general suspicion, and aggressive narratives can raise fears of escalation in the context of conflict. This has especially been the case with deployment missions to Ukraine.

Consequently, governments have increasingly opted to share information about their deployment missions, aiming to demonstrate that they serve diverse purposes and unfold in various political contexts, many of which are civilian rather than military. In this paper, we draw on publicly available information to explore deployment missions.

It attempts to address the definitional blurriness of the concept and refines the tool for cybersecurity support deployments. To this end, we have compiled a list of 16 deployment cases from recent years (provided in the annex), which have been analyzed using a purpose-developed framework.

Key findings

The utilization of deployments as a means of enhancing cybersecurity is communicated by some countries through proactive inclusion in strategic and policy documents or cooperation agreements. However, these communications primarily focus on the overarching goals of deployments without delving into the specific details of individual missions. Detailed information, such as deployment activities, the resources involved, and team configurations, is typically shared after the fact through press releases, via media coverage, or at cybersecurity events. This approach is largely driven by strategic considerations. Governments are cautious about revealing their intent to adversaries, as public disclosure could prompt them to remove their adversarial capabilities, enhance their concealment of access, or learn from observing the deployed team, thus strengthening their ability to evade detection in the future.

- Governments generally view deployment as one of several tools at their disposal to improve cybersecurity.
- Deployment is typically seen as a method for pursuing a variety of objectives in the fields of cybersecurity, cyber defense, and resilience, such as taking preventive action, assisting with incident response skills, and learning more about a threat actor.
- In addition to the objective of enhancing cybersecurity, deployments can serve other purposes, such as economic, national security, defense, or foreign policy considerations. For example, governments utilize deployments to foster cooperation and at the same time, prevent cyber incidents.
- The specific objective of a deployment determines its unique configuration. For instance, capability-building deployments (in which one state enables another to conduct a vulnerability assessment) entail different requirements than scenarios in which a state simply requests that another perform a preventive activity without gaining the skills necessary for future endeavors. Consequently, different types of deployments, potentially involving distinct personnel and timing, are necessary to address these varying needs.
- Deployments can also aim to enhance another state's capacity to perform specific tasks. For instance, in the aftermath of a specific incident, a government may seek to acquire a particular capability to bolster its effectiveness in responding to similar situations.
- The cases examined also shed light on the diverse policy domains in which cybersecurity support deployments have been observed, including foreign policy, national security policy, and defense policy. In numerous instances, there are indications that deployments arise from long standing operational, policy, diplomatic, or military partnerships.

- Government entities assume various roles within deployments. They may serve as funders, providing financial support for the deployed resources. In addition, government staff can play a dual role, either by being deployed to execute specific activities or by overseeing the implementation of the deployed resources. Furthermore, certain government entities exercise a level of control, supervision, and instruction, directing or managing the deployed resources and/or activities.
- Examining the role of governments can provide insights into the setup of deployment missions, the involvement of non-government stakeholders, and the level of control exerted by the deploying government.
- The concept of "trust" is crucial in the context of cybersecurity deployments. Two dimensions are relevant: trust among government officials, which is necessary to facilitate deployments, and trust among professionals involved in implementing cyber activities during deployments. These dimensions are separate but can reinforce each other and interrelate, albeit through different mechanisms.
- During deployments, capacity building takes place as teams engage in active implementation, allowing them to develop new skills and enhance their existing capabilities. This process applies to the supporting country and the supported country. Cybersecurity deployments are dynamic learning environments where continuous learning and skill development occur rather than mere provision-based arrangements.

Within the policy community, there is growing interest in cybersecurity support deployment. If such deployment missions are to become even more widely used, we recommend five practical considerations for governments, based on current empirical research:

1. Consider the "Principle of Permission"
2. Consider different forms of how permission can be granted
3. Clearly state the need for cybersecurity support in the request
4. Consider who could best provide the requested support
5. Consider who should request support.

Furthermore, we recommend that countries considering the use of deployments in the future carefully consider their objectives and the specific contexts in which they intend to employ such missions. Policy makers should also give careful thought to how they can foster a sense of "personal trust" among the practitioners involved. This involves considering with whom and in what manner personal-level relationships can be established. For instance, forming joint teams and showcasing individual competences and skills can serve as effective trust-building measures

before or during specific deployments. Additionally, practitioners should be actively engaged from the early stages of discussions surrounding potential cybersecurity support deployments.

To advance research in this field, we suggest that the analytical framework for cybersecurity support deployments developed in this paper be expanded. This can be achieved by incorporating additional dimensions, such as mapping the diverse legal frameworks that govern deployments, and by including more cases from a wider range of countries.

Table of Contents

Introduction

Governments are increasingly recognizing that improving cybersecurity requires partnered and cooperative responses. This has led to an increased need for cooperation among governments and other non-government stakeholders. "We need to cooperate more" or "We need to cooperate on this" have become common phrases in cybersecurity dialogues. Different types of cooperation have emerged in this context, such as information-sharing agreements, the exchange of liaison officers, or the establishment of task forces.[1] Several studies have examined these types of cooperation and government involvement, including cooperation between governments and the private sector and cooperation among Computer Security Incidents Response Teams (CSIRTs)[2] worldwide. **This paper explores a particular form of cooperation that can be considered a type of "deployment". Governments have increasingly turned to this approach in recent years, yet it remains a relatively understudied method of collaboration, and its characteristics have analytically hardly been understood.**

Originally a military term, deployment refers to "the movement of troops or equipment to a place or position for military action."[3] To analyze this tool in the field of cybersecurity, the working definition in this paper for "cybersecurity support deployment" is as follows:

The working definition for Cybersecurity Support Deployment is

"Military and/or civilian cybersecurity support deployments can be applied when cybersecurity professionals from one country provide support to another based on their government's decision involving a cybersecurity-related activity or resources, such as hardware and software."

1 See the recent joint statement on the SNAKE takedown: NCSC (2023) *UK and allies expose snake malware threat from Russian Cyber Actors*. NCSC. (n.d.). https://www.ncsc.gov.uk/news/uk-and-allies-expose-snake-malware-threat-from-russian-cyber-actors

2 A general term that refers to a group that deals with computer security incidents. To minimize the damage caused by computer security incidents, they collect and analyze incident-related information, vulnerability information, and predictive information of cyberattacks, consider solutions and measures, and handle the incidents: Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRTS and Global Cybersecurity: How technical experts support science diplomacy. *Global Policy*, *9*, 60–66. https://doi.org/10.1111/1758-5899.12625

3 *Deploy verb - definition, pictures, pronunciation and usage notes: Oxford Advanced American Dictionary at Oxfordlearnersdictionaries.com*. deploy verb - Definition, pictures, pronunciation and usage notes | Oxford Advanced American Dictionary at OxfordLearnersDictionaries.com. (n.d.-a). https://www.oxfordlearnersdictionaries.com/definition/american_english/deploy

Deployments can be physical—meaning that persons actually travel to a requesting country; deployment can also mean that support is provided digitally[4] or by sending materials. It is important to understand that deployments can happen below the threshold of armed conflict and for objectives other than incident response. The public and policy debates surrounding cybersecurity support deployments need to acknowledge the nature and scope of government deployment missions, with the aim of providing cybersecurity support and the possible objectives and activities of such deployments.

Some cybersecurity support deployments (deployments/CSDs) in the context of the Russian invasion of Ukraine have received the most media attention. However, upon reflection, it is striking how vague the public discourse has been regarding the definition and scope of cybersecurity support deployments. It is important to understand that deployments to build trust and capacity were ongoing long before the invasion. However, most media attention was dedicated to the deployments in January and February 2022, after Ukraine experienced various cyber incidents targeting its government services[5]. Following a request from Ukraine, several countries considered deployments. Practitioners focused on practical questions and discussed possible preventive IT security measures[6]. In the media, the deployments were depicted as a means to "fend off Russian hackers,"[7] "fight Russian cyberattacks," and "ward off Russian cyberattacks, which had previously accompanied Moscow's kinetic combat."[8] The public debate surrounding cybersecurity support for Ukraine at that time revealed a general lack of understanding of the nature and scope of government deployment missions. To make effective use of deployments, decision-makers and those who influence policy decisions must grasp the purpose(s) of cybersecurity support and the possible objectives and activities of such deployments.

Requesting support from other countries for matters of national security by inviting their experts can be a sensitive issue. It is discussed, developed, and applied by practitioners, and its implementation mostly occurs behind the scenes, away

4 In cybersecurity support deployments, digital support can also be considered deployment due to the domain-specific possibility of remotely conducting actions within the supported governments' IT infrastructure from anywhere in the world.

5 In a letter to EU leaders, Kyiv's Foreign Minister Dmytro Kuleba says that they "welcome deployment to Kyiv" of a team of experts to evaluate "vulnerabilities of our key computer networks and systems." Kuleba also requested "additional technical equipment and software for strengthening the cybersecurity infrastructure" from the EU. Cerulus, L. (2022, February 22). *EU to mobilize cyber team to help Ukraine fight Russian cyberattacks*. POLITICO. https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/

6 For instance, Lithuania's Vice Minister of Defense Margiris Abukevicius at the time stated that "European officials will work out the details with Ukraine on how many and which experts it will devote to the operation." Cerulus, L. (2022, February 22). *EU to mobilize cyber team to help Ukraine fight Russian cyberattacks*. POLITICO. https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/

7 Cerulus, L. (2022, February 22). *EU to mobilize cyber team to help Ukraine fight Russian cyberattacks*. POLITICO. https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/

8 ByAFP. (2022, February 25). *Cyber attack risks poised to Soar as Russia attacks Ukraine. SecurityWeek.* https://www.securityweek.com/cyber-attack-risks-poised-soar-russia-attacks-ukraine/

from public scrutiny. Governments that have engaged in this type of cooperation have typically avoided publicizing it. This is not totally surprising, because until recently, deployments in the field of cybersecurity were a topic almost exclusively reserved for a group of highly specialized experts in different countries. This lack of detailed information has certainly contributed to the undifferentiated nature of the ensuing debates. Insufficient knowledge and misunderstandings of the concept of deployment missions can, however, lead to general suspicion, and aggressive narratives can raise fears of escalation in the context of conflict.

Governments have thus started to increasingly provide information about their deployment missions in order to demonstrate that they are carried out for various reasons and within diverse political contexts, with many of them civilian rather than military. By doing so, governments contribute to better-informed and more differentiated public debates. **We compiled a list of 16 cybersecurity support deployments conducted by different nations in recent years (please refer to the complete list in the annex). Please note that the list of cases in the annex is not comprehensive, as numerous cases may remain undisclosed, and our focus is limited to publicly available data.**

We attempt to address the definitional blurriness and help sharpen the tool of cybersecurity support deployments by analyzing the cases. To this end, we developed an analytical framework that was implemented in this paper.

Part 1 of the paper presents a summary of the key findings derived from analyzing the practices in the case studies. Part 2 offers practical considerations in response to the increasing prevalence of deployments, including practical recommendations for policymakers who plan to initiate and request cybersecurity support. Finally, part 3 touches on analytical dimensions that warrant further investigation and could be incorporated into the existing analytical framework.

Framework for Analysis

The following **analytical framework was developed** to gain a better understanding of the current practice of CSDs. The framework was employed to analyze cases that met two criteria: sufficient publicly accessible information and alignment with the working definition.

The table presented below provides a summary of the analyzed dimensions and the insights derived from answering associated questions. For instance, examining the requesting or deploying entity—whether it is a government institution or another actor—can shed light on the policy domain(s) in which deployment is employed. In addition, the role that government entities play can determine the role that other non-government stakeholders play in the course of a deployment. Specific activities can reveal what objectives or needs the deployment aims to address. **Future analysis may encompass additional dimensions, as we discuss in the outlook section (part 3).**

Framework for analyzing cases of cybersecurity support deployment

Relevant questions about deployment(s)	Analytical conclusions about deployment
• Who requested the support/ deployment, through what ways (civil defense, technical support, etc.)? • Who organized or conducted it? • Which government entity communicates in public about the deployment?	• Indication of what policy field the deployment falls into • Indication of the policy context
• What are the broader strategic goals of the deployment? • What are the specific objective(s) of the deployment?	• Indication of what policy area, e.g., national security, economic policy, foreign policy, or defense policy • Indication of expectations • Indication of what activities and resources the deployment entails
• What role(s) do(es) the government entit(ies) take on in the deployment? For example, provide funding (for what?), provide staff members, exercise control and supervision?	• Indication of the degree of responsibility and accountability of the governments involved • Indication of which non-government stakeholders are involved, their roles, and responsibilities • Indication of specific setup • Indication of activities and resources during the deployment
• Which activities are undertaken as part of the deployment?	• Indication of what setup is the best fit, e.g., joint team, bilateral, multilateral, remote, or in person
• What led to the deployment? For example, previous relationships	• Indication of expectations • Indication of the wider policy context of the deployment

Part 1: Cybersecurity Support Deployment—Findings Regarding Current Practice

Part 1 of the paper summarizes some of the main findings derived from the analysis of the 16 cases (see the list here).

1. Deployments are a tool for achieving *different* cybersecurity, cyber defense, and resilience objectives.

When the way government entities communicate during or in the wake of deployment missions is examined, two observations can be made. First, governments generally view deployment as one of several tools at their disposal. Second, deployment is typically seen as a method for pursuing a variety of objectives in the fields of cybersecurity, cyber defense, and resilience[9]. In May 2022, the United States communicated that it had funded the deployment of cybersecurity experts to Ukraine specifically "to improve cybersecurity information sharing in Ukraine's financial services sector"[10]—an objective that can be broadly described as promoting cooperation and assisting in building cybersecurity capabilities. In another case, Canada and Latvia shared with the public via a press statement in January 2022 that the deployment of Canadian experts aimed at "identifying and eliminating technical and coordination 'bottlenecks'" with the broader aim of enhancing "cyber protection capacity on both sides."[11] The objectives were twofold: to assist in building cybersecurity capabilities and promote cooperation. In November 2022, Lithuanian-led (CRRTs)[12] developed within the European Union (EU) Permanent Structured Cooperation (PESCO) framework in the area of security and defense were deployed in support of Moldova, and in March 2023, CRRT experts were sent to Mozambique in support of EU Training Mission MOZ[13].

9 NIST SP 800-39 under Information System Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. Editor, C. C. (n.d.). *Resilience - glossary: CSRC*. CSRC Content Editor. https://csrc.nist.gov/glossary/term/resilience#:~:text=with%20mission%20needs.-,Source(s)%3A,naturally%20occurring%20threats%20or%20incidents

10 Office of the Spokesperon. (2022, May 11). *U.S. support for connectivity and Cybersecurity in Ukraine - United States Department of State*. U.S. Department of State. https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/

11 Ministry of Defence of the Republic of Latvia, Media Relations. (n.d.). *Latvia and Canada join forces in a national information and communication technology threat hunting operation*. Aizsardzības ministrija. https://www.mod.gov.lv/en/news/latvia-and-canada-join-forces-national-information-and-communication-technology-threat-hunting

12 Ministry of National Defence of the Republic of Lithuania, Media Relations. (2023, March 30). *Lithuanian-coordinated EU Cyber Rapid Response Teams – incident response with the EU and in support of EU partners and military missions.* https://kam.lt/en/lithuanian-coordinated-eu-cyber-rapid-response-teams-incident-response-with-the-eu-and-in-support-of-eu-partners-and-military-missions/

13 Ministry of National Defence of the Republic of Lithuania, Media Relations. (2023, March 30). *Lithuanian-coordinated EU Cyber Rapid Response Teams – incident response with the EU and in support of EU partners and military missions.* https://kam.lt/en/lithuanian-coordinated-eu-cyber-rapid-response-teams-incident-response-with-the-eu-and-in-support-of-eu-partners-and-military-missions/

The deployments had the same goal: They were supposed to conduct a vulnerability assessment, which is a proactive measure to look for vulnerabilities and, in this way, contribute to the requesting entity's increased resilience. This is an activity in which the broader objective is to take preventive action. Looking at our compilation of cases, and specifically at how governments have communicated the objectives of their deployment missions, deployments are considered a potential policy option to achieve different goals related to cybersecurity and resilience in current practice. Moreover, one deployment can cover one or more objectives. Looking at the goals shows that governments use deployments strategically, considering their own goals and those of the requesting country. Therefore, some of these goals can have, in addition to improving cybersecurity, economic, national security, defense, or foreign policy interests in mind. With deployments, governments aim, for example, to promote cooperation while preventing cyber incidents. Developing human resources abroad from an economic viewpoint could be a goal to decrease staff shortages for international businesses, while the same deployment also builds the requesting country's capacities. These synergies are explored in more depth in the next finding. Examining all the cases revealed that the communicated objectives fit into these broader categories.

Government Cybersecurity Support Deyplopment Goals

Building Capabilities To assist in building cybersecurity capabilities	**Prevention** To take preventive actions	**Cooperation** To promote cooperation	**Incident Response** To assist with specific incident response skills
Human Resources To improve available human resources	**Threat Analysis** To learn more about a threat (abroad)	**Cyber Defense** To assist with cyber defense activities during crises or specific threats	**Resources** To increase available resources

Reference: Schuetze, Daukšienė (2023) "Cybersecurity Support Deployments: An emerging cooperative approach", SNV

2. Cybersecurity deployment is a tool in different policy fields.

The goals for a particular deployment mission and the institution that communicates those goals hint at the policy fields in which the mission operates. To highlight this, we discuss three examples in more detail. For other examples, please check the annex.

Two examples highlight that previous U.S. cybersecurity support deployments to other countries have been within different policy fields.

Case Example: U.S. cybersecurity support deployments in national security and defense policy

Case Countries	Time	Entity That Deploys	Entity That Receives	Specific Activities of Support	Derived Goals of Support	Indicated Policy Field(s)	Sources
United States–22 countries	Since 2018	U.S. Cyber National Mission Force (CNMF)	Different Countries Military and Civil Federal Entities	*"hunting for malicious cyber activity and identifying vulnerabilities on networks"* *"provided technical findings (...) enabling the partner to take steps toward bolstering their network defense"*	• To learn about a threat abroad • To assist with cyber defense activities during crises or specific threats • To take preventive actions	National Security Policy Defense Policy	Link to Media Link Press Release

Since 2018, U.S. military operators have been deployed to 20 countries, usually close allies, in Europe, the Middle East, and the Indo-Pacific region.[14] Looking at Cyber Command's operating concept of persistent engagement explains that deployment is one tool in this strategy. Persistent engagement is a strategic element of the U.S. national security strategy, which "prescribes that the United States defend forward both geographically (beyond Department of Defense networks) and temporally (ahead of adversary exploitation) to enable anticipatory resilience in domestic and foreign partner networks."[15] Major General William Hartman, commander of the Cyber National Mission Force, said in March 2022 at the Air Force Association's Air Warfare Symposium that deployments by the Cyber National Mission Force have the following policy goals: first, "to ensure that we can actively engage with our adversaries in foreign space"[16] (to defend forward); second, "to reinforce our

14 Gordon Corera In (2022, October 30) Inside a US military cyber team's defence of Ukraine - BBC News. (n.d.). Retrieved May 25, 2023, from https://www.bbc.com/news/uk-63328398.

15 Michael P. Fischerkeller, E.O.G. (2022) *Persistent engagement in cyberspace is a strategic imperative*, *The National Interest*. Available at: https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/persistent-engagement-cyberspace (Accessed: 26 May 2023).; The US practice of hunt forward is in part also a trust building mechanism with the host country. In this paper this goal is subsumed under "improve cooperation" and the matter of trust is discussed in chapter four and seven. See also Robson, K. (2023) *US sends more cyber forces overseas to fight hackers*, *Verdict*. Available at: https://www.verdict.co.uk/us-sends-more-cyber-forces-overseas-to-fight-hackers/ (Accessed: 26 May 2023).

16 Pomerleau, M. (2022, March 4). *Cyber Command has deployed to nations 27 times to help partners improve cybersecurity.* https://fedscoop.com/cyber-command-has-deployed-to-nations-27-times-to-help-partners-improve-cybersecurity/

relationships with our partners and allies"[17] (to promote cooperation); and finally, "to ensure that whatever our adversaries are doing in their near abroad, they can't do that back here in the United States"[18] (to learn about a threat (abroad)). The goals suggest that deployments are seen as an instrument for the United States to achieve its own defense and national security policy objectives, such as resilience, and those of its partners. Deployment is a common means used in U.S. defense policy to learn about adversaries abroad and to assist other countries in identifying adversarial activity. Therefore, deployments by the U.S. Cyber Command Cyber National Mission Force can also be connected to the field of defense and national security policy. However, deployments do not necessarily have to be connected to the field of defense policy. They can also be connected to a country's foreign policy.

Case Example: U.S. cybersecurity support deployments in national security and foreign policy

Case Countries	Time	Entity That Deploys	Entity That Receives	Specific Activities of Support	Derived Goals of Support	Indicated Policy Field(s)	Sources
United States–Ukraine	Press release from May 2022	U.S. Treasury Department	National Bank of Ukraine	*"improve cybersecurity information sharing in Ukraine's financial services sector"* *"long-term projects to ensure cyber resilience"*	• To take preventive actions • To assist in building cybersecurity capabilities	Foreign Policy, National Security Policy	Link to Press Release
United States–Ukraine	Press release from May 2022	U.S. Agency for International Development (USAID)	Essential Service Providers in Ukraine	*"hands-on support"* *"identify malware and restore systems"*	• To assist with specific incident response skills	National Security Policy Foreign Policy	Link to Press Release

In May 2022, the United States published that the U.S. Agency for International Development (USAID) assisted with CSD in Ukraine. USAID is an independent agency of the U.S. federal government that "leads the U.S. Government's international

17 Pomerleau, M. (2022, March 4). *Cyber Command has deployed to nations 27 times to help partners improve cybersecurity.* https://fedscoop.com/cyber-command-has-deployed-to-nations-27-times-to-help-partners-improve-cybersecurity/

18 Pomerleau, M. (2022, March 4). *Cyber Command has deployed to nations 27 times to help partners improve cybersecurity.* https://fedscoop.com/cyber-command-has-deployed-to-nations-27-times-to-help-partners-improve-cybersecurity/

development and disaster assistance through partnerships and investments."[19] USAID funded "technical experts" to provide "hands-on support to essential service providers within the Ukrainian government including government ministries and critical infrastructure operators to identify malware and restore systems after an incident has occurred."[20] In this case, the deployment was connected to U.S. foreign policy because the agency administering the deployment "supports the objectives of the National Security Strategy and other strategic documents, such as the Department of State-USAID Joint Strategic Plan, that aim to strengthen our diplomatic and development capabilities to better meet our foreign policy goals."[21] The policy field of not only the deploying countries matters. Deployments can be connected to the policy field of the requesting or partnering countries, which may differ. This support was connected to Ukraine's cybersecurity policy goals.[22]

Deployments usually benefit all contributing parties in some shape or form. The new cybersecurity strategy of the United States, published 2 March 2023, supports this analysis, as the new strategy states that "providing this support will not only assist with partner recovery and response, but will also advance U.S. foreign policy and cybersecurity goals."[23]

These examples highlight how the communicated objectives and the government entities involved hint at which policy area a specific deployment is connected to. Countries that aim to use deployments in the future should consider which objectives they aim to achieve and in what context they want to use deployments. Japan, for example, has used deployments in the context of foreign policy, national security policy, and economic policy but not specifically in a defense policy setup. For deploying countries and requesting countries, these are important considerations, as they determine the framework under which the deployment happens. The policy area can also determine the setup and activities during a deployment (how the deployment actually looks) and who can request and/or who decides which entity can deploy. These practical considerations are discussed in part 2.

19 USAID. (n.d.). *Mission, Vision and Values | About Us | U.S. Agency for International Development*. U.S. Agency for International Development. https://www.usaid.gov/about-us/mission-vision-values

20 Office of the Spokesperon. (2022, May 11). *U.S. support for connectivity and Cybersecurity in Ukraine - United States Department of State*. U.S. Department of State. https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/

21 USAID. (n.d.). *Policy*. U.S. Agency for International Development. https://www.usaid.gov/policy

22 Oleksii Tkachenko (2017, July 6) *Cybersecurity in Ukraine: National Strategy and international* cooperation. Retrieved May 25, 2023, from https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation.

23 US National Cybersecurity Strategy. (2023). Retrieved May 25, 2023, from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, page 31

3. Governments take on different roles in deployments, which influence the roles of non-government stakeholders involved in the deployment.

Looking at the different roles governments assumed in our compilation of exemplary cases, we can identify three different roles government entities[24] could take during a deployment: Government entities can fund the deployed resource, government staff can be either deployed to implement a certain activity or handle the implementation of a deployed resource, and government entities can have a certain level of control and supervise instructing, directing, or controlling the deployed resource and/or activity[25].

Examining the role of governments can provide some clues about the setup of deployment missions and tell a story about the amount of control the government that deploys cybersecurity support has in the actual implementation. In certain cases, the control and supervision were very clear. Examples of government staff involvement in which the deploying entity had control and supervision over the activities are the deployments of the U.S. Cyber Command Cyber National Mission Force. A close working relationship and observation of tasks were mentioned in a BBC report: "Cyber professionals from both countries sat side by side, looking for adversary activity and identifying vulnerabilities."[26] Another example in which government involvement was clear is when France's cybersecurity agency, ANSSI, supported, and assisted in detention, analysis, and cybersecurity remediation in Montenegro.[27] In other cases, staff of more than one government have shared implementation, supervision, and control of the cybersecurity support, such as when EU Member States (Belgium, Croatia, Estonia, Lithuania, the Netherlands, Poland, Romania, and Slovenia) agreed to assist the Government of Moldova with a vulnerability assessment as part of the CRRT (developed within the PESCO framework)[28].

In other cases, it was harder to assess from public communication. For example, when government entities appear as funders of the deployment, their involvement

24 Consider "whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State." Art. 4 of the Articles of State Responsibility

25 See language in Art. 8 of the Articles on State Responsibility

26 Gordon Corera In (2022, October 30) *Inside a US military cyber team's defence of Ukraine* - BBC News. (n.d.). Retrieved May 25, 2023, from https://www.bbc.com/news/uk-63328398.

27 Mubariz Zaman (2022, August 29) Montenegro thanks France for assistance following cyberattacks. (n.d.). Retrieved May 25, 2023, from https://thediplomaticinsight.com/montenegro-thanks-france-for-assistance-following-cyberattacks.

28 Ministry of National Defence of the Republic of Lithuania, Media Relations. (2023, March 30). *Lithuanian-coordinated EU Cyber Rapid Response Teams – incident response with the EU and in support of EU partners and military missions* .https://kam.lt/en/lithuanian-coordinated-eu-cyber-rapid-response-teams-incident-response-with-the-eu-and-in-support-of-eu-partners-and-military-missions/

in instructing, directing, or controlling the deployed resource and/or activity is more difficult to determine in comparison to when government staff are also implementing the activity.

When a government takes on the role of a funder of the deployment, but its staff is not involved in the implementation, then control and supervision of the implementation could be taken on by staff of non-government stakeholders, such as private companies, freelance technical experts, NGOs, or the receiving governments. This also applies when governments that fund the deployment of hardware or software leave the implementation to the requesting countries' entities. In such cases, the government may still control or supervise the type of hardware and software deployed. However, the receiving government or a private sector stakeholder actually operationalizes the specific activity.[29] One example of this is the cooperation between the U.S. Treasury Department and the National Bank of Ukraine (NBU). The U.S. government agency funded the activity, but the Software Engineering Institute's (SEI's), a Federally-Funded Research and Development Center (FFRDC) at Carnegie Mellon University, staff was deployed. Therefore, the SEI's staff had more control and supervision of the deployed activity, together with the NBU's CSIRT. In Japan, for example, the Japan International Cooperation Agency (JICA) manages capacity-building projects with partner countries but may resort to external experts from, for example, JPCERT/CC, which is organized as an independent nonprofit organization for specific deployment missions[30].

Another example in which government and private entities had to work closely together was documented by the *Financial Times* in March 2022. It described a situation in which the Ukrainian national police, alongside other Ukrainian government arms, were facing a massive onslaught of "distributed denial-of-service [DDoSs] attacks". The U.S. government contacts familiar with the situation in Ukraine at the time contacted Fortinet, a Californian cyber security group that sells a "virtual machine" designed to counter just such an attack. The article described the process: "funding was approved within hours and the U.S. Department of Commerce provided clearance within 15 minutes. Within eight hours of the request, a team of engineers had installed Fortinet's software onto Ukrainian police servers to fend off the onslaught, said a person familiar with the rapid-fire operation."[31]

29 Depending on the context, it can become relevant whether the non-government stakeholders are instructed, directed, or controlled by a state. If they are, their activities are considered an act of state and in that particular case, as an act of state support (Art. 8 Articles on State Responsibility).

30 JICA (2021, June 18). CSIRT Training by JPCERT/CC | Technical Cooperation Projects .... (n.d.). Retrieved May 25, 2023, from https://www.jica.go.jp/project/english/vietnam/052/news/general/210618.html.l

31 Mehul Srivastava and Madhumita Murgia in London, Hannah Murphy in San Francisco (2022, March 9) *The secret US mission to bolster Ukraine's cyber defences ahead of* ..... Retrieved May 25, 2023, from https://www.ft.com/content/1fb2f592-4806-42fd-a6d5-735578651471.

In summary, government involvement can vary, and the varying roles influence the setup of a specific support mission. Government roles shape the roles that non-government stakeholders and the receiving government play in a deployment mission.

4. Deployments emerge from long-term operational, policy, diplomatic, or military partnerships.

In many cases, there are indications that deployments emerge from a longer-term operational, policy, diplomatic, or military partnership. The Canadian deployment of cybersecurity support to Latvia was directly connected to an existing relationship between Canadian government agencies and the Latvian CSIRT. Canada had been present in Latvia with an enhanced forward presence battle group. Having engagements before deployment of support was credited for the success of the deployments, said Brigadier-General Dave R. Yarker, Canadian Joint Forces Cyber Component, commander, at the Cybersecurity conference CyberChess 2022: "if trust doesn't exist two people sitting right next to each other will get nowhere."[32]

A relationship can also be built outside the defense policy context. France and Montenegro had established a close diplomatic relationship before the deployment of cybersecurity support. They signed a letter of intent[33] just months before the deployment that stated their intention to build a cybersecurity capacity center in Montenegro with the assistance of France. Although the public documents did not indicate any intended deployments at that time, their previous collaboration on cybersecurity may have influenced Montenegro's decision to seek France's support and France's willingness to provide it.

5. Deployments require organizational- and personal-level trust.

When discussing deployments, the concept of "trust" plays an important role. Trust can be broken into two separate dimensions: trust between government officials needed for deployments and trust between professionals implementing the cyber activity during a deployment. The dimensions are distinct and can reinforce and interrelate, but they involve different mechanisms. For example, "even countries allied to the U.S. can be nervous about allowing the U.S. to root around inside sensitive government networks," the BBC report about the so-called "hunt forward"

32 CERT.LV (2022, October 21). *BGen. Dave R. Yarker, CyberChess 2022* https://www.youtube.com/watch?v=RiWX5uuVjNs

33 Office of the Deputy Prime Minister/University of Montenegro (2022, March 29. *Letter of Intention by University and Government of Montenegro to .....* Retrieved May 25, 2023, from https://www.gov.me/en/article/the-letter-of-intention-by-the-university-of-montenegro-and-the-government-of-montenegro-to-the-government-of-france-montenegro-to-be-the-place-for-the-regional-center-for-cyber-security-and.

deployments of the United States stated.[34] Considering this is important because organizational- and policy-level trust does not translate automatically to the actual implementers' personal need to trust. In cybersecurity support deployments, therefore, the preferred approach is to interact in person and not (only) digitally, or at least to know each other very well[35]. For example, the activity of the deployments can require becoming a team. This setup is chosen to build trust due to the nature of the activities, which are highly sensitive. In such a context, working closely together is a necessity. Therefore, local partners "sometimes sit with U.S. teams around in conference rooms observing closely to make sure nothing untoward is going on."[36] Another reason is that in the cybersecurity community, probably more than in other domains, "pretty much no one believes your accreditations, no one believes that you can do what you say you can do until you show them," said Canadian Brigadier-General Dave R. Yarker[37]. Therefore, Yarker concluded "that it is important that we take the time to show each other competence, to build that trust in each other's ability, to do what we say we're going to do."[38] The personal-level relationships formed during actual "on the ground" deployments, however, can also serve as door-openers for further partnerships and/or repeated deployments.

For policy makers, it is therefore important to think about with whom and what setup these personal-level relationships can be formed. For example, forming a joint team and demonstrating each other's competences and skills to build trust can happen before or during specific deployments. A case in which a joint team was built as part of a specific deployment is the cooperation among Latvia, Canada, Belgium, and the EU in December 2022[39]. CERT.LV, the Information Technology Security Incident Response Institution of Latvia, which operates under the Ministry of Defence of the Republic of Latvia, communicated that it "conducted a threat hunting operation to identify adversarial presence on Latvian critical infrastructure. To conduct this operation, the CERT.LV reached out to international partners to form a joint cyber team with the Canadian Military Cyber Forces, the Communications Security Establishment's Canadian Centre for Cyber Security (Cyber Centre), the Belgian Military Cyber Command, and the European Union Agency for Cybersecurity (ENISA)."[40]

34 Gordon Corera In (2022, October 30) Inside a US military cyber team's defence of Ukraine - BBC News. (n.d.). Retrieved May 25, 2023, from https://www.bbc.com/news/uk-63328398.
35 Also see https://onlinelibrary.wiley.com/doi/epdf/10.1111/1758-5899.12625
36 Gordon Corera In (2022, October 30) Inside a US military cyber team's defence of Ukraine - BBC News. (n.d.). Retrieved May 25, 2023, from https://www.bbc.com/news/uk-63328398.
37 CERT.LV (2022, October 21). *BGen. Dave R. Yarker, CyberChess 2022* https://www.youtube.com/watch?v=RiWX5uuVjNs
38 CERT.LV (2022, October 21). *BGen. Dave R. Yarker, CyberChess 2022* https://www.youtube.com/watch?v=RiWX5uuVjNs
39 CERT.LV (2022, December 1). *Latvia, Canada, Belgium, and ENISA Join Forces in a ...* - CERT.LV. (n.d.). Retrieved May 25, 2023, from https://cert.lv/en/2022/12/latvia-canada-belgium-and-enisa-join-forces-in-a-cyber-threat-hunting-operation.
40 CERT.LV (2022, December 1). *Latvia, Canada, Belgium, and ENISA Join Forces in a ...* - CERT.LV. (n.d.). Retrieved May 25, 2023, from https://cert.lv/en/2022/12/latvia-canada-belgium-and-enisa-join-forces-in-a-cyber-threat-hunting-operation.

In contrast, the CRRT developed within the PESCO framework was formed as a multinational team before specific deployments occurred. The CRRT is a team that consists of government experts from different participating countries (Belgium, Croatia, Estonia, the Netherlands, Lithuania, Poland, Romania, and Slovenia).[41] The setup by default is multilateral, and deployments can occur "as a response to cyber incidents and crises as well as a preventive measure (for vulnerability assessments, election monitoring, etc.)"[42]. Trust in each other's skills was central to the mission; therefore, the CRRTs Project is based on sharing the strengths of each participant, best practices, and procedures as well as experience between the participating Member States. This means that each Project Member State before the beginning of the CRRT rotation delegates cyber expert(s) with specific profiles or skill sets, contributing to a full-spectrum CRRT, able to respond to a variety of challenges and ready on standby. Therefore, decision-makers may need to increase their awareness of the skillset and support activities possible, as this can be helpful for identifying a suitable setup and context for deployments.

6. Building capabilities or increasing capacities are deployment objectives.

Capability building or increasing capacity are deployment objectives to consider.

Objective 1: To assist in building a certain capability

First, let's examine how capacity building can be an objective of deployments. Cybersecurity support can be deployed for various reasons, such as responding to an incident or identifying threats. Looking at the cases, there are two objectives in which deployments are conducted due to capacity building, but their context and setup differ. One is to assist in building a certain capability. These are mostly deployments that focus on enabling another government to get better at a certain cybersecurity activity. In that case, the deployment often features in a country's foreign policy strategy or in a Memorandum of Understanding between governments defining the tools of cooperation. Deployments may be featured next to other formats, such as information sharing. If assisting in building a certain capability is the main reason for deployment, this impacts the format and activities chosen. The deployment should then have the goal of enabling the receiving government to carry out the activities by themselves in the future.

A good example is Japan's support of Vietnam with the DDoS Attack Mitigation System[43]. The Project on Capacity Building for Cyber Security in Vietnam procured IT equipment, such as servers, displays, disks, and workstations. In addition, training

41 CRRT. (n.d.). Retrieved May 25, 2023, from https://crrts.eu.
42 CRRT. (n.d.). Retrieved May 25, 2023, from https://crrts.eu.
43 JICA. (2021, March 13). *Installation of Equipment for DDoS Attack Mitigation System*. JICA. https://www.jica.go.jp/project/english/vietnam/052/news/general/210313.html

was provided to strengthen the capacity of operators and maintenance managers to use the system. The project identified "dispatching experts" and deploying "equipment" as a means of achieving a certain objective, such as enhancing the capacity of proactive services[44].

Consider the fictitious example of state A, which is about to hold an election. Its government asks state B for support for a vulnerability assessment. If state A and state B do not agree that building the capability "vulnerability assessment" is part of the deployment, then state B's support team carries out the assessment and shares its findings with state A. State A could then take care of fixing the vulnerabilities. However, it would not have learned how to carry out vulnerability assessments in the future, as this may require extra training as part of the deployment or transparency into how state B came to the conclusion. For state B, teaching state A how to carry out vulnerability assessments would be a different deployment mission with different objectives and a different setup. Capability-building deployments, such as enabling another state to conduct a vulnerability assessment, are a different need and require a different format of deployment, possibly different people and possibly different timing; for example, the deployment needs to be expressed much earlier. **The benefit of including capacity building as an objective in deployments is that they would follow the same practical considerations as deployments for other reasons** (see part 2).

Example Objective 2: To increase capacities at a specific time e.g., to assist with incident response skills

Second, increasing a government's capacity to do something can also be an objective for deployments. For example, during a specific incident, a government asks for a specific capability to increase its capacity to respond. According to the CSIRT Services Framework, in such a context capacity is understood as "the number of simultaneous process-occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion."[45]

For example, increasing capacity could be an objective for deployment during an incident. When France assisted Montenegro, during the deployment, they increased Montenegro's capacity to respond.

44 JICA. (2019, March 8). *Outline of the Project*. JICA. https://www.jica.go.jp/project/english/vietnam/052/outline/index.html

45 FIRST (no date) CSIRT services framework version 2.1, FIRST. Available at: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1 (Accessed: 26 May 2023).

7. Capacity building and closer cooperation are benefits of deployments.

Public statements indicate that, in some of the cases analyzed in this paper, deployments have led to closer partnerships and cooperation. **The formalized nature of deployments offers a framework that sets clear expectations and accountability due to the specific goals and activities agreed upon. This makes deployments different from other forms of cooperation that are less formalized and demand less confidence in each other's capabilities.** During deployments, capacity is built because "the doing" enables teams to develop new skills and thus build capacity that did not exist before. This works for the supporting country and the supported country. Cybersecurity deployments are dynamic learning environments, not simply "provision" environments. Although initially Canada intended to support Latvia, Brigadier-General Dave R. Yarker noted that this came with "an implication that Canada has come to do something for the CERT," but "that's not a one-way-exchange, in fact the nature of the ultimate team sport is that it is absolutely a two-way-exchange. Canada has gained enormously from its interactions here in Latvia."[46] Yarker mentioned that the deployment was key to building some of Canada's expertise in training their operators due to the opportunities in Latvia.

Some cases indicated that what starts as a deployment of cybersecurity support could lead to a much closer relationship with advantages for both countries. Therefore, the deployment of cybersecurity support can be a supporting partnership between the two countries—something to consider when requesting support.

8. Governments communicate more details after missions have ended.

Governments have communicated about deployments of cybersecurity support before and after the mission. Public communication seldom occurs during a mission. The use of deployments as a tool to further cybersecurity is communicated by some countries proactively in strategic and policy documents[47] or cooperation agreements[48] stating mostly only the goals of the deployments in general without providing details of individual deployments. Specific details, such as deployment

46 CERT.LV (2022, October 21). *BGen. Dave R. Yarker, CyberChess 2022* https://www.youtube.com/watch?v=RiWX5uuVjNs

47 US National Cybersecurity Strategy. (2023). Retrieved May 25, 2023, from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, page 31
Japan MOFA (2021, December 14) *(provisional translation) Basic Policy on Cybersecurity Capacity Building Support for Developing Countries*. Available at: https://www.mofa.go.jp/files/100347812.pdf (Accessed: 26 May 2023).

48 Permanent structured cooperation (PESCO) (no date) *Cyber Rapid Response Teams and Mutual Assistance in Cyber Security* (CRRT) *PESCO*. Available at: https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/#:~:text=Permanent%20Structured%20Cooperation%20(PESCO),-Deepen%20defence%20cooperation&text=CRRTs%20will%20be%20equipped%20with,assessments%20and%20other%20requested%20support (Accessed: 26 May 2023).

activities, resources involved, and team setups, are communicated mostly afterward in press releases,[49] in the media,[50] or at cybersecurity events.[51] Detailed communication after a deployment and not prior may be due to strategic reasons. For example, to be most effective, governments would not want their adversary to know they are hunting or proactively seeking to strengthen a network they may have penetrated because the adversary might remove their adversarial capabilities, improve concealment of access, or importantly learn by watching the deployed team, thus strengthening their ability to avoid detection in the future. These key operational security reasons may be why communication after deployment is more common.

9. Communication about deployments matters.

Communication about deployments matters for different reasons, depending on the target audience. For governments or non-government stakeholders directly involved in the implementation of cybersecurity support, communication can clarify mutual expectations. For these stakeholders, communication helps place the deployment in a broader policy context. The cases show that both sides connect deployments to their specific needs before or after a specific deployment occurs.

A good example is the cybersecurity support deployment between Japan and Indonesia aimed at increasing the availability of human resources in cybersecurity via their capacity building cooperation project which was initiated in 2019 and is as of writing extended to 2024[52]. Japan's goals for such deployment are communicated broadly in their cyber foreign policy strategy. The strategy states that "the global lack of advanced experts in the cybersecurity field has presented a major challenge for Japanese businesses operating in the ASEAN region in terms of securing the necessary human resources."[53] The strategy concludes that "we will develop human resources to support the activities of Japanese businesses overseas, including

49 See examples in the annex: Canada-Latvia; MOD.LV (2022, January 7) *Latvia and Canada join forces in a national information and communication technology threat hunting operation*, Aizsardzī bas ministrija. Available at: https://www.mod.gov.lv/en/news/latvia-and-canada-join-forces-national-information-and-communication-technology-threat-hunting (Accessed: 26 May 2023).; USA-Ukraine Office of the Spokesperon. (2022, May 11). *U.S. support for connectivity and Cybersecurity in Ukraine - United States Department of State*. U.S. Department of State. https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/; JICA (2022, October 4) *Signing of Record of Discussions on Technical Cooperation Project with Mongolia: Project for Development of Human Resources in Cybersecurity*. JICA.

50 See example in the annex: USA-Ukraine - Gordon CoreraIn (2022, October 30) Inside a US military cyber team's defence of Ukraine - BBC News. (n.d.). Retrieved May 25, 2023, from https://www.bbc.com/news/uk-63328398.; France - Montenegro in annex; Mubariz Zaman (2022, August 29) *Montenegro thanks France for assistance following cyberattacks*. (n.d.). Retrieved May 25, 2023, from https://thediplomaticinsight.com/montenegro-thanks-france-for-assistance-following-cyberattacks.

51 CERT.LV (2022, October 21). *BGen. Dave R. Yarker, CyberChess 2022* https://www.youtube.com/watch?v=RiWX5uuVjNs

52 JICA (2019, May 22) *Outline of the project*, *JICA*. Available at: https://www.jica.go.jp/project/english/indonesia/023/outline/index.html (Accessed: 26 May 2023).

53 MOFA (2021, December 14) *(provisional translation) Basic Policy on Cybersecurity Capacity Building Support for Developing Countries*. Available at: https://www.mofa.go.jp/files/100347812.pdf (Accessed: 26 May 2023)

ASEAN, over the medium to long term, and create an environment that facilitates understanding of diverse cultures and acceptance of foreign resources at Japanese businesses through industry-government-academia collaboration."[54] Thus, in this case, Japan stated its intentions for possible deployments in the cooperation agreement with Indonesia but also embedded it into the strategy giving more context.

Indonesia, the country receiving cybersecurity support in this case, has identified a matching need - addressing the lack of human capital capable of securing Indonesia's cybersecurity landscape. This is discussed in the development of a national cyber security of the country since at least 2017 and is an ongoing need.[55] In this policy context, Japan and Indonesia have set up a mutual cooperation agreement in which cybersecurity support deployment is identified as an instrument to "provide cyber security human resources"—their shared strategic goal[56].

For the media and journalists, communication about deployment matters for other reasons, for example, because it is their job to inform the public. The public might want to know about deployments because they want to understand their government's policies toward other countries, or because they are interested in other governments' involvement in their national infrastructure. Researchers and think tankers, however, need information about deployment missions to analyze the empirical and theoretical implications of this form of cybersecurity support. For governments not involved in the deployment, communication may be a way of understanding other states' activity. To leave less room for (mis)interpretation, governments have recently shared much more detailed information about their deployments. For example, when Croatia received support from the United States, Daniel Markić, the head of Croatia's security and intelligence agency, stated for a news report afterward that "the hunt was thorough and successful, and we discovered and prevented malicious attacks on Croatian state infrastructure."[57] He added, "We were able to offer the US a new 'hunting ground' for malicious actors and share our experience and acquired knowledge."[58] What can be concluded from the analysis is that the country that deploys and the one that receives support show a strategic alignment, and that deployment can be mutually beneficial.

54 MOFA (2021, December 14) *(provisional translation) Basic Policy on Cybersecurity Capacity Building Support for Developing Countries*. Available at: https://www.mofa.go.jp/files/100347812.pdf (Accessed: 26 May 2023).

55 Irnasya Shafira (2021) *Analyzing Indonesia's National Cybersecurity Strategy*, *Analyzing Indonesia's National Cybersecurity Strategy : Center for Digital Society*. Available at: https://cfds.fisipol.ugm.ac.id/2021/07/28/analyzing-indonesias-national-cybersecurity-strategy/ (Accessed: 26 May 2023).

56 JICA (2019, May 22) *Outline of the project*, *JICA*. Available at: https://www.jica.go.jp/project/english/indonesia/023/outline/index.html (Accessed: 26 May 2023).

57 Gordon CoreraIn (2022, October 30) Inside a US military cyber team's defence of Ukraine - BBC News. (n.d.). Retrieved May 25, 2023, from https://www.bbc.com/news/uk-63328398.

58 Gordon CoreraIn (2022, October 30) Inside a US military cyber team's defence of Ukraine - BBC News. (n.d.). Retrieved May 25, 2023, from https://www.bbc.com/news/uk-63328398.

Part 2: Future Cybersecurity Support Deployments—Practical Considerations

In the policy community, there is increasing interest in using cybersecurity support deployments. If they are to become even more widely used, some practical considerations based on the available empirical research could be taken into account. We see them only as a starting point and welcome contributions from others that may add, disagree, or aim to highlight some of the practices in future dialogues.

We gathered five practical considerations for requesting and providing cybersecurity support.

1. Consider the "principle of permission".

All states are equal before international law, regardless of the size of their territory, population, economy, or military might—the principle of sovereign equality, written in the UN Charter,[59] dictates. Following this principle, states are in control of affairs within their borders and are protected against undue interference from the outside. This means that, in cybersecurity support deployments, permission must be granted by the hosting state before cybersecurity-related activities can start in its territory. This also applies to remote activities that involve access to the state's critical infrastructure. Permission essentially means that there is a legal basis[60] for the activities involving the respective states. Therefore, the following recommendations focus on the role of the requesting, or, in other words, the hosting state, as its needs primarily dictate the conduct of cybersecurity activities.

2. Consider different forms for how permission can be granted.

How permission is granted by the hosting state to conduct cybersecurity activities in its territory might vary significantly, however. Permission can be actively expressed by the hosting state in time of need through a request or invitation, either proactively to address cybersecurity-related threats or in the case of a significant cybersecurity incident or crisis. In the same manner, potential service providers could offer their support, for example, for capacity-building purposes based on an ongoing cooperation agreement. What the request or the permission should entail and in what form it should be expressed, once again, is totally up to the parties involved and will depend on the context. Permission could be part of the ongoing engagement,

59 UN Charter, Article 2.

60 Eglė Daukšienė (former: Vasiliauskaitė), Tadas Šakūnas (n.n.), *Legal Memo for Mutual Assistance in Cyber Security Legal Basis for the CRRTs' Operations*. Available at: https://kam.lt/wp-content/uploads/2022/03/legal-memo.pdf (Accessed: 26 May 2023). p. 11

such as a bilateral or multilateral cooperation agreement, as one of the planned activities,[61] or it could be requested ad hoc based on the needs of the hosting state[62]. If there is no formal agreement process, states that seek cybersecurity support and states that offer cybersecurity support can initiate conversations and explore potential options for request formats, for example, in cybersecurity policy dialogues. However, although it does not matter who initiates the support, the activity must be commonly agreed upon in advance.

3. Clearly state the "need" for cybersecurity support in the request.

The needs of the requesting entity set the basis for the provision of the cybersecurity support that follows. The needs may also be determined in consultation with possible deploying states, as the requesting state may not know in all cases what is available. Therefore, the most important question to answer when considering cybersecurity support is the following: What is needed (i.e., what kind of cybersecurity support or service)? Is it a case of a vulnerability assessment, capacity building, or cybersecurity incident management? In any case, the needs and some context of the host environment should be clearly stated. For example, if it is a case of a cybersecurity incident, details should be given about what happened, what systems are affected, the extent of the impact thus far, what mitigating measures were applied, and the expected outcome of the requested cybersecurity support.

Why do the mentioned aspects matter as part of the necessary knowledge before cybersecurity activities can begin? Everything else, meaning the nature, the conduct, and the success of the cybersecurity activities, will depend on it: the types of expertise that will be selected for the requested activity, the number of personnel, the duration of the deployment, the selection of tools, etc. A clear understanding of the situation essentially allows cybersecurity professionals to do their job. This will contribute significantly to increased effectiveness, efficiency, reaction-ability, accountability, and, overall, capacity building. However, if these aspects are not clearly stated before the cybersecurity activities are conducted, the cybersecurity support implementers will not know exactly what is being asked of them, the expected outcomes, and the boundaries of the requested activity. At best, this would be an obstacle to effective time and human resource management on both ends. At worst, the cybersecurity activity could bring about outcomes that were not intended by the requesting party. It is important to note that the situation and the needs of the requesting entity might change, to which the incident response team should be able to adapt. The changed objectives or outcomes of the requested support should be clearly stated by the requesting entity before further steps are taken.

61 See the cases Canada–Latvia in annex
62 See the cases France–Montenegro and CRRT–Ukraine in annex

Finally, what matters is not only clearly indicated and assessed expected outcomes but also the ability to fulfill them. In other words, before the requested activity is conducted, the added value of cybersecurity support providers should be considered and assessed in light of potential negative consequences.

4. Consider who could best provide the requested support.

To whom permission is granted to conduct cybersecurity support in a state's territory depends on the needs and the political context of the respective states. The request can be initiated in another state based on strong ongoing bilateral cooperation. In the same manner, the respective state can request a multinational cybersecurity capability provided by its partners. Cybersecurity support can also be provided, and consequently, permission can be granted to EU institutions, international organizations, or a private sector entity. As shown in the cases, the role of governments can differ on a case-by-case basis, and can be influenced by the political and organizational compatibility of the states. Moreover, the role of government entities may affect the involvement of non-government stakeholders in the support mission. Of course, the availability of cybersecurity experts, especially in a volatile environment often further influenced by political winds, can never be fully guaranteed. Therefore, it is always useful to consider possible alternatives for the provision of the requested support. Thinking about how the need for support relates to different policy goals of states can also assist in finding a good match. As shown in the analysis, governments evaluate whether the deployment aligns with their overall cybersecurity goals and then assess which agency or entity, either internal or external to their cybersecurity architecture, can provide (or has the skill set to provide) the necessary support.

The following are the determining factors for the choice of the potential support implementer:

1. **the specificity of the technical expertise needed and**
2. **the existing relationship, taking into account the trustworthiness and commitment of the partner.**

These two factors are especially important when considering the conduct of cybersecurity activities of a sensitive nature, which would require access to the systems of the state's critical infrastructure. Additional steps can be taken as safeguards, such as the requirement that experts have clearances[63] or sign non-disclosure agreements before the activities are conducted. Nevertheless, in any case, trust will always be the basis of such cooperation.

63 Eglė Daukšienė (former: Vasiliauskaitė), Tadas Šakūnas (n.n.), *Political 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*. Available at: https://kam.lt/wp-content/uploads/2022/03/CRRT-2018.pdf (Accessed: 26 May 2023). p. 24

5. Consider who can request support.

What is important to consider is who has the authority to request support on behalf of a state or state entity in the first place. Depending on the nature of the cybersecurity support, the process demands the right institution or person who would have a mandate to act on behalf of the respective state in the field of cybersecurity. If cybersecurity is consolidated in a respective state, it could be an institution that has the highest authority in the field, such as the Ministry of Defense, Ministry of Economy, Ministry of Communications, and so on. Examples of such an institution include national CERT/CSIRT, for example, identified as a Single Point of Contact according to the NIS2 Directive[64]. In the same manner, if a number of institutions share equal authority in the field of cybersecurity, a combination could have the authority to request cybersecurity support depending on the situation, for example, sectorial CERT, if there is a cybersecurity incident involving that particular sector. In any case, the aspect of authority or a selection of authorities must be discussed and determined before the respective state entity asks for support. As can be seen in the cases, the stakeholders requesting support can differ considerably. For more sensitive support, this aspect could be included as part of a national cybersecurity law, policy, or strategy identifying which institution(s) would have the authority to ask for international support and in which cases of need.

The role of the national authority matters not only as part of the requester of the support but also as the enabler of its fulfillment. A good example is the case of Ukraine, which, having requested support from different countries, coordinated more than one deployment on the ground at once: "The Ukrainian National Cybersecurity Coordination Center, established in 2016, has played a key role in synchronizing these disparate operations and actors."[65] Practical aspects to consider, which would enable the coordination of efforts with regard to the provision of cybersecurity support, include the following: The cybersecurity specialists will need to have a point of contact who is familiar with the local IT infrastructure[66] as well as someone who would be able to support them logistically[67] so that the specialists can focus solely on their task at hand.[68]

64 DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

65 Beecroft , N. (2022) *Evaluating the international support to Ukrainian Cyber Defense*, *Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (Accessed: 26 May 2023).

66 Eglė Daukšienė (former: Vasiliauskaitė), Tadas Šakūnas (n.n.), *Political 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*. Available at: https://kam.lt/wp-content/uploads/2022/03/CRRT-2018.pdf (Accessed: 26 May 2023). p. 24

67 Eglė Daukšienė (former: Vasiliauskaitė), Tadas Šakūnas (n.n.), *Political 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*. Available at: https://kam.lt/wp-content/uploads/2022/03/CRRT-2018.pdf (Accessed: 26 May 2023). p. 24

68 Beecroft , N. (2022) *Evaluating the international support to Ukrainian Cyber Defense*, *Carnegie Endowment for International Peace*. Available at: https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322 (Accessed: 26 May 2023).

Part 3: Outlook

In the previous chapters, we presented the results of our empirical analysis of cases of cybersecurity support deployments (see annex). As mentioned, it is important to bear in mind that this list of cases is by no means exhaustive, as some deployment missions have not or have not been fully publicly disclosed. Through the employment of the analytical framework outlined in this paper, our objective was to refine the concept of "deployment" and differentiate it from other forms of cybersecurity cooperation. The analysis aims to contribute to a systematic understanding of this cybersecurity support deployment, which can also be of value in future policy discussions. Moreover, several practical considerations emerged that warrant discussion for future setups. We offer two key recommendations to facilitate further study and enhance the practical implementation of deployments.

Recommendation 1:
Expand the framework of analysis and consider more cases.

We recommend using the analytical framework that was applied in this study. However, we suggest expanding it by adding more dimensions. This expansion can prove beneficial in informing the formulation of policies related to the implementation of CSDs. Cases from countries should be included, as their objectives may differ from those examined in this paper.

Here are some examples of questions that could be incorporated into the analytical framework:

- What are the potential political and operational risks of engaging in a specific cybersecurity deployment mission?
- What was the existing legal foundation for deployment?
- Which international law framework is applicable? For example, state responsibility, international liability, or non-interference?
- Have the countries used deployments in other contexts (e.g., outside cybersecurity) before?
- What does the relationship between government and non-government stakeholders look like in more detail?
- How are control and supervisory power shown?
- Should there be a clearer differentiation between deployments and other cooperation tools (e.g., training cooperation and exercises)?
- How could deployments that are managed by an international intermediary (e.g., the Global Forum on Cyber Expertise or ENISA) look?

Recommendation 2:
Bridge the gap between policymakers and practitioners to develop beneficial deployment missions.

When policymakers consider using deployments to achieve cybersecurity objectives, it is important to consult with practitioners during the setup process. Such consultation can provide valuable insights into feasible activities and available resources, and may offer guidance on areas where trust and relationships already exist. Considering the necessity of establishing "personal trust" among practitioners, discussing the most effective approach to achieve a specific objective from the outset can be beneficial. For example, forming a joint team and demonstrating each other's competences and skills to build trust can be undertaken before or during specific deployments.

Annex: Cases of Cybersecurity Support Deployment

Overview of cybersecurity support analyzed (analytical conclusions were drawn from public communication)

Case Countries	Time	Entity That Deploys	Entity That Receives	Specific Activities of Support	Public Communication About Support	Derived Goals of Support	Indicated Policy Field(s)	Set-Up / Involvment Non-Gov Stakeholders	Role of Government Communicated	Sources
USA – 27 countries	Since 2018	U.S. Cyber National Mission Force (CNMF)	Different Countries Military and Civil Federal Entities	*"hunting for malicious cyber activity and identifying vulnerabilities on networks"* *"provided technical findings (...) enabling the partner to take steps toward bolstering their network defense"*	Before and After Deployment via Press Releases and Media	• To learn about a threat abroad • To assist with cyber defense activities during crises or specific threat • To take preventive actions	National Security Policy Defense Policy	Bilateral	Staff Supervision and Control	Link to Media Link Press Release Link Press Release
EU Member States (Belgium, Croatia, Estonia, Lithuania, the Netherlands, Poland, Romania, Slovenia) - EU Member States and Partners, EU institutions, bodies and agencies, CSDP Missions and Operations	Since 2018	CRRT (developed within PESCO framework)	EU Member States and Partners, EU institutions, bodies and agencies,CSDP Missions and Operations	*"preventive actions and carry out cyber-vulnerability assessments"* *"facilitate the ability to share best practices and will to improve the efficiency of using technological and human resources"* *"assistance in managing a cyber-incident or carrying out prevention (vulnerability assessments, elections observation, etc.)"*	Before Deployment via Media and Policy Documents and After Deployment via Press Release	• To take preventive actions • To assist with specific incident response skills • To promote cooperation	National Security Policy Defense Policy	Multilateral	Funding Staff Supervision and Control	Link to Media Link to Media Link to Website Link to Press Release

Case Countries	Time	Entity That Deploys	Entity That Receives	Specific Activities of Support	Public Communication About Support	Derived Goals of Support	Indicated Policy Field(s)	Set-Up / Involvment Non-Gov Stakeholders	Role of Government Communicated	Sources
Japan - Indonesia	Since 2018	JICA Japan	University of Indonesia, Ministry of Communication and Information Technology	*"training program"* *"open source cyber security tools"* *"open courseware"* *"a network"*	Before and During Deployment via Project Website	• To improve human resources available • To assist in building cybersecurity capabilities	Foreign Policy	Bilateral Academia	Funding Staff Supervision and Control	Link to Website
Japan - Vietnam	2019-2022	JICA Japan	Ministry of Information Communication (MIC), Authority of Information Security(AIS)	*"Training in Vietnam, Training in Japan"* *"Equipment: Servers, Network equipment, Software, etc. Mission team dispatch"* *"Expand reactive infrastructure (e.g. DDoS attack mitigation) in AIS"* *"Expand proactive infrastructure (e.g. network monitoring) in AIS"*	Project Website Project News Updates	• To assist in building cybersecurity capabilities • To take preventative actions	Foreign Policy National Security Policy	Bilateral Japanese Experts for example from JPCERT/CC	Funding, Supervision and Control, Staff	Link to Project Website Example Deployment of Equipment and Training
USA – Singapore	Since 2021	U.S. Treasury Department	Monetary Authority of Singapore	*"staff training and study visits"* *"competence-building activities"* *"cybersecurity exercises"*	Before Deployment via Press Release	• To assist in building cybersecurity capabilities • To promote cooperation	Foreign Policy National Security Policy	Bilateral	Funding Staff	Link to Press Release

Case Countries	Time	Entity That Deploys	Entity That Receives	Specific Activities of Support	Public Communication About Support	Derived Goals of Support	Indicated Policy Field(s)	Set-Up / Involvment Non-Gov Stakeholders	Role of Government Communicated	Sources
USA - Ukraine	Oct 2021 – Feb 2022	U.S. Cyber Command	Ukrainian Cyber Command	*"conducted defensive cyber operations"* *"looking for adversary activity and identifying vulnerabilities"* *"remote analytic and advisory support"*	After Deployment via Press Release and Media	• To assist with cyber defense activities during crises or specific threat • To take preventative actions • To learn more about a threat (abroad)	Defense Policy National Security Policy	Bilateral Critical Infrastructure Providers	Staff Supervision and Control	Link to Press Release Link to Media Link to Media Link to Media
Canada - Latvia	Jan 2022	Canadian Cyber Command	CERT.LV	*"joint real-time Threat Hunting Operations"* *"tested and developed the existing procedures"* *"identifying and eliminating technical and coordination 'bottlenecks'"* *"enhance its analytical capacity"*	After Deployment via Press Release	• To assist in building cybersecurity capabilities • To promote cooperation • To assist with cyber defense activities during crises or specific threat	Defense Policy National Security Policy	Bilateral	Staff Supervision and Control	Link to Press Release
USA - Ukraine	Press release from May 2022	U.S. Treasury Department	National Bank of Ukraine	*"improve cybersecurity information sharing in Ukraine's financial services sector "* *"long-term projects to ensure the cyber resilience"*	Press Release After Deployment	• To take preventive actions • To assist in building cybersecurity capabilities	Foreign Policy, National Security Policy	Bilateral Critical Infrastructure Provider NGO	Funding	Link to Press Release

Case Countries	Time	Entity That Deploys	Entity That Receives	Specific Activities of Support	Public Communication About Support	Derived Goals of Support	Indicated Policy Field(s)	Set-Up / Involvment Non-Gov Stakeholders	Role of Government Communicated	Sources
USA - Ukraine	Press release from May 2022	U.S. The Agency for International Development (USAID)	Different entities in Ukraine	*"6,750 emergency communications devices, including satellite phones and data terminals"*	Press Release After Deployment	• To assist with cyber defense activities during crises or specific threat • To increase available resources	National Security Policy Foreign Policy	Bilateral Private Sector Critical Infrastructure Providers	Funding Control and Supervision	Link to Press Release
USA – Ukraine	Press Release from May 2022	U.S. The Agency for International Development (USAID)	Essential Service Providers in Ukraine	*"hands-on support"* *"identify malware and restore systems"*	Press Release After Deployment	• To assist with specific incident response skills	National Security Policy Foreign Policy	Bilateral Independent Technical Experts	Funding	Link to Press Release
EU Member States (Belgium, Croatia, Estonia, Lithuania, the Netherlands, Poland, Romania, Slovenia)	2022	CRRT (developed within PESCO framework)	Government of Moldova	*"vulnerability assessment"*	After Deployment via Press Release	• To take preventative action	National Security Policy	Multilateral	Funding Staff Supervision and Control	Link to Press Release
France, Slovenia – Montenegro, Western Balkan	Since 2022	France Ministry for Europe and Foreign Affairs, Slovenian Foreign Ministry	Center for Cybersecurity Capacity Building in the Western Balkans	*"providing training"* *"train the trainer model"* *"exchange of best practices"*	Before Deployment via Press Release	• To promote cooperation • To assist in building cybersecurity capabilities	Foreign Policy National Security Policy	Multilateral tbd	Funding	Link to Press Release Link to Press Release

Case Countries	Time	Entity That Deploys	Entity That Receives	Specific Activities of Support	Public Communication About Support	Derived Goals of Support	Indicated Policy Field(s)	Set-Up / Involvment Non-Gov Stakeholders	Role of Government Communicated	Sources
France – Montenegro	Aug-Sept 2022	National Agency for the Security of Information Systems (ANSSI)	Government of Montenegro	*"recovery efforts"* *"support and assist in the detention, analysis and cybersecurity remediation"*	Before Deployment via Media Coverage and After Deployment via Press Release	• To assist with specific incident response skills	National Security Policy Foreign Policy	Bilateral	Staff Supervision and Control	Link Media Link Media Link Press Release
Japan - Mongolia	Oct, 2022	JICA Japan	Government of Mongolia	*"implementing education programs"* *"conducting train-the -trainer programs"*	Press Release Before Deployment	• To improve human resources available • To assist in building cybersecurity capabilities	Foreign Policy, National Security Policy, Economic Policy	Bilateral Private Sector Academia	Funding, Supervision and Control, Staff	Link to Press Release
Canada, Belgium, EU - Latvia	Dec 2022	Canadian Military Cyber Forces, the Communications Security Establishment's Canadian Centre for Cyber Security (Cyber Centre), the Belgian Military Cyber Command, and the European Union Agency for Cybersecurity (ENISA).	CERT.LV	*"threat hunting operation"* *"verify cyber threat intelligence sharing and incident response procedures"* *"develop operational capabilities and enhance interoperability"* *"defend systems based on the collected threat intelligence"*	After Deployment via Press Release	• To promote cooperation • To learn more about a threat (abroad) • To take preventative actions • To assist with cyber defense activities during crises or specific threat	Defense Policy National Security Policy	Multilateral	Staff Supervision and Control	Link to Press Release

Case Countries	Time	Entity That Deploys	Entity That Receives	Specific Activities of Support	Public Communication About Support	Derived Goals of Support	Indicated Policy Field(s)	Set-Up / Involvment Non-Gov Stakeholders	Role of Government Communicated	Sources
EU Countries (Belgium,Croatia, Estonia, Lithuania, the Netherlands, Poland, Romania,Slovenia)	Press release from 2023	CRRT (developed within PESCO framework)	European Union Training Mission in Mozambique	*"vulnerability assessment"*	After Deployment via Press Release	• To take preventaive action	National Security Policy	Multilateral	Funding Staff Supervision and Control	Link to Press Release

About Stiftung Neue Verantwortung

Stiftung Neue Verantwortung (SNV) is a non-profit think tank at the intersection of technology and society. At SNV's core is a methodology of collaborative development of policy proposals and analyses. SNV experts do not work alone – they develop and test ideas together with representatives from politics and public administration, technology companies, civil society and academia. Our experts work independently of interest groups and political parties. We guarantee our independence through diversified financing, comprised of contributions from different foundations, state and corporate actors.

About Transatlantic Cyber Forum

To further policy research in the area of international cybersecurity and provide concrete recommendations, the Stiftung Neue Verantwortung (SNV) established The Transatlantic Cyber Forum (TCF) in January 2017. TCF is an intersectoral network and currently consists of more than 150 practitioners and researchers from civil society, academia and private sector working in various areas of transatlantic cybersecurity policy.

About the Authors

Julia Schuetze is project director for cybersecurity policy and resilience at Stiftung Neue Verantwortung e.V. where she chaired the Transatlantic Cyber Forum working group on deployment of cybersecurity support. Since 2017, she has managed different projects for SNV, focused on comparative cybersecurity policy, European cybersecurity policy, cyber operations against election processes and cyber resilience of local government entities. She also designs and implements multi-stakeholder cybersecurity policy exercises.

Eglė Daukšienė is an advisor at Cyber Security and IT Policy Group at the Ministry of National Defence of the Republic of Lithuania. Eglė has worked in the field of Cyber over the past six years, managing the development of Lithuanian-led multinational cyber capability, developed within the PESCO project "Cyber Rapid Response Teams (CRRT) and Mutual Assistance in Cybersecurity". In addition to capacity building, Eglė has specialised in large-scale cyber incident and crisis management, application of international law to cyber, national and EU policy making as well as more broadly international cooperation in cybersecurity.

Contact the author

Julia Schuetze
Project Director Cybersecurity Policy and Resilience
jschuetze@stiftung-nv.de
Twitter: @juschuetze

Imprint

Stiftung Neue Verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Alina Siebert