CYBERDEFENSE REPORT

Cyber Rapid Response Teams
Structure, Organization, and Use Cases

Taylor Grossman

Zürich, November 2023
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zürich

ETH zürich

Available online at: https://css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Taylor Grossman

ETH-CSS project management: Stefan Soesanto, Project Lead Cyberdefense; Andreas Wenger, Director of the CSS.

Editor: Stefan Soesanto
Layout and graphics: Miriam Dahinden-Ganzoni

© 2023 Center for Security Studies (CSS), ETH Zürich

DOI: 10.3929/ethz-b-000643234

Table of Contents

1 Introduction

Cyber rapid response teams are becoming an increasingly prevalent form of incident response and mitigation at the national and supranational level. Nation-states and international organizations have begun building out teams to efficiently manage incidents and leverage expertise across borders. Over the past two decades, NATO and the EU have each developed their own rapid response teams to manage and mitigate the rise in cyberattacks, including incidents that cut across borders and affect international partners. Yet, many questions remain regarding a team's composition, organizational and legal structures, as well as their overall efficacy.

Under the EU's Permanent Structured Cooperation (PESCO) arrangement – which is part of the EU's Security and Defense Policy (CSDP) – Lithuania and several other member states created the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) project in 2018. These teams are generally collaborative between military and civilian organizations. Lithuania leads the CRRT PESCO project, which currently consists of seven participating states (Belgium, Croatia, Estonia, the Netherlands, Poland, Romania, and Slovenia) and five observer states (Finland, France, Greece, Italy, and Spain). The leadership of the CRRT rotates annually among the participating states, with Lithuania maintaining the co-lead function. Although the project has conducted several cyber exercises since its inception, the first CRRT was activated in late February 2022 in support of Ukraine but was never deployed due to the Russian ground invasion.[1]

The inaugural exercises in 2018 – named Cyber Shield / Amber Mist – revealed key weaknesses in the CRRT arrangement, including member states' uncertainty regarding their own cyber response expertise.[2] CRRT membership has also shifted over the past five years: Spain and Finland moved from active membership to observer status, while Germany was an observer but has now left the project entirely. Belgium and Slovenia recently joined the CRRT team as participating states, and in early 2023 Czechia and Denmark also expressed interest in joining the project. Overall, the CRRT project is intended to create a shared repository of cyber expertise and capabilities, and ultimately to foster expanded EU resilience in the face of cyberattacks.[3]

The CRRT has yet to be deployed to deal with an acute or ongoing crisis. However, in the past 18 months, the project has made significant strides, sending teams into Moldova in November 2022 and Mozambique in March 2023 to perform vulnerability assessments and help improve cyber defenses.[4] Indeed, the CRRT project is consistently praised as one of the most advanced and successful PESCO projects.[5]

Yet, the CRRT project has not been able to deliver on its original promise – responding quickly to EU member states or partners in times of great need. The CRRT teams continue to be a valuable symbol of EU solidarity and support for partner nations, but they have not yet achieved the "rapid response" capabilities that they were set out to provide.

In 2012, NATO established a Cyber Rapid Reaction Team (RRT) to increase cohesion across the alliance and aid member states in the event of cyberattacks of "national significance."[6] Since the release of NATO's 2010 strategic concept, cyber defense has become an increasingly pronounced element of the organization's outlook.[7] In 2014, NATO declared that a cyberattack could be considered an armed attack, triggering the collective defense clause enshrined in Article 5 of the North Atlantic Treaty, if said incident reaches a certain threshold of destruction. In July 2016, NATO made clear its understanding of cyberspace as an operational domain, and at the 2018 Brussels Summit the alliance declared

[1] "EU Cyber Rapid Response Teams to Support Ukraine," government, *Ministry of National Defence, Republic of Lithuania* (blog), February 23, 2022, https://kam.lt/en/eu-cyber-rapid-response-teams-to-support-ukraine/.

[2] "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security, Key Roles and Procedures for the CRRTs' Operations, Lessons Learnt from the Cyber Shield / Amber Mist 2018 Exercise" (Lithuania: Ministry of National Defence of the Republic of Lithuania, 2018).

[3] "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security Legal Basis for the CRRTs' Operations" (Lithuania: Ministry of National Defence of the Republic of Lithuania, 2018).

[4] James Osborne and Joseph Jarnecki, "Battening Down the Hatches: Moldova's Cyber Defence," *RUSI*, August 10, 2023, https://www.rusi.org/explore-our-research/publications/commentary/battening-down-hatches-moldovas-cyber-defence; Monika Benkler, "Deploying CSDP Missions to Counter Hybrid Threats - EUPM Moldova: First of Its Kind" (Tech Pops, August 4, 2023), https://tech-blog.zif-berlin.org/deploying-csdp-missions-counter-hybrid-threats-eupm-moldova-first-its-kind; "Lithuanian-Coordinated EU Cyber Rapid Response Teams - Incident Response with the EU and in Support of EU Partners and Military Missions," *Ministry of National Defence Republic of Lithuania*, March 30, 2023, 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/.

[5] "PESCO Projects Adapt and Accelerate Amid Shifting European Security Landscape, EU Report Finds," *European Defence Agency*, July 11, 2023, Online edition, https://eda.europa.eu/news-and-events/news/2023/07/11/pesco-projects-adapt-and-accelerate-amid-shifting-european-security-landscape-eu-report-finds.

[6] "NATO Rapid Reaction Team to Fight Cyber Attack," *North Atlantic Treaty Organization* (blog), March 13, 2012, https://www.nato.int/cps/en/natolive/news_85161.htm.

[7] "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization" (Lisbon, Portugal: NATO, November 19, 2010), https://www.nato.int/cps/en/natohq/topics_82705.htm.

that cyber defense is an explicit component of its collective defense mission.[8] Finally, in 2020, NATO unveiled a strategy to use any (and all) capabilities to counter a cyberattack – including air, naval, or land forces.[9]

On the offensive side, cyber operations have remained siloed within the alliance. While many military capabilities provided by a member state – aircraft, warships, etc. – are handed over to the control of a NATO military commander in times of conflict, cyber operations remain the purview of the member state. Critics have noted that this command-and-control structure creates a black box when cyber capabilities are invoked, whereby NATO military commanders request a cyber effect be rendered but remain in the dark about its operational realities.[10] Problems of transparency and effectiveness could easily arise, as NATO leaders may be unaware of potential second- and third-order effects resulting from a specific requested cyber operation.

On the defensive side, NATO's Cyber Rapid Reaction Team program also remains opaque. While the original intention was to integrate member state capabilities into small, nimble units capable of quick deployment to any member state in need, no RRT has ever been activated through this system. NATO has done very little to publicize the program or its uses.[11]

First, this report outlines the general structure of a cyber rapid response team and the limits and benefits of different styles of construction. Next, it delves into two in-depth case studies: the EU CRRT and NATO's RRT. Finally, it examines several incidents where teams were considered for international deployment. Ultimately, neither CRRT nor RRT has been used to answer calls for crisis state assistance.[12]

[8] "Brussels Summit Declaration" (Brussels, Belgium: North Atlantic Council, July 11, 2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

[9] Jamie Shea, "NATO: Stepping up Its Game in Cyber Defence," *Cyber Security* 1, no. 2 (May 10, 2017): 165–74.

[10] Shea.

[11] "Cyber Defence," North Atlantic Treaty Organization, April 4, 2023, https://www.nato.int/cps/en/natohq/topics_78170.htm; Senior NATO Official, Author Interview on NATO Cyber Rapid Response Teams, interview by Taylor Grossman, phone, March 22, 2023.

[12] Senior NATO Official, Author Interview on NATO Cyber Rapid Response Teams; Author interview with senior PESCO CRRT team official, interview by Taylor Grossman, Telephone, November 15, 2022.

2 Background: Structuring a Multinational Rapid Response Capability

Crisis management systems have often emerged to face new types of threats, consolidating response capabilities, and streamlining best practices. In the field of cybersecurity, computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs) "provide an important sense-making capacity in cyber crises."[13] CERTs and CSIRTs first emerged in the late 1980s in response to the Morris worm, an internet worm deliberately designed to spread rapidly and infect as many machines as it could. Although its creator, Robert Morris, had launched the worm as an "innocuous experiment," he ended up crashing about 10% of existing Internet-connected computers.[14]

The Defense Advanced Research Projects Agency (DARPA), an offshoot of the US Department of Defense (DoD) and an early Internet pioneer, established the first ever CERT.[15] The Computer Emergency Response Team Coordinating Center (CERT/CC) was set up through the Software Engineering Institute (SEI), a Federally Funded Research and Development Center (FFRDC), at Carnegie Mellon University. FFRDCs are specialized private sector organizations with unique partnerships with their sponsoring federal agency or department. In the case of SEI, that sponsor is the DoD.[16] The first CERT, therefore, emerged in an interesting position—outside and adjacent to federal organizations, but still deeply intertwined with their work.

The new CERT/CC was established to serve as "the first emergency responders for cyberspace."[17] The organization quickly found it had its work cut out for it: CERT/CC received its first emergency call only hours after the press release announcing its existence had gone out.[18]

Many institutions in the United States were quick to follow the DoD's lead, establishing their own CERT infrastructure in the next 12 months. In 1990, CERT/CC and ten other similar incident response teams established a "CERT System" to improve coordination across computer emergencies. The newly established system was seen as US-dominated, and so was renamed and expanded into the Forum of Incident Response and Security Teams (FIRST) in 1992.[19]

Yet, outside of the United States, CERTS spread much more slowly. In 1993, when FIRST was formally announced by the US National Institute of Standards and Technology (NIST), only five of the 21 participating organizations were located outside of the US (the UK, France, the Netherlands, Denmark, and Germany). The CERT/CC system "had a very pragmatic reason to help teams get started in other countries: hackers around the world were launching attacks on US networks."[20]

By the mid-1990s, CERTs had become more common throughout Europe. While FIRST was still dominated by US organizations, by 1996, 13 of its 59 members were in Europe (representing 22 percent of its roster).[21]

Multinational institutions, however, tended to lag behind state and sector-led initiatives. A EuroCERT pilot project was launched from 1997-1999 by TERENA, the Trans-European Research and Education Networking Association.[22] The EuroCERT pilot project faltered, however, as participating teams were unsure whether the organization should function as a loose coordinator or as an active incident responder in its own right.[23] The project lead resigned shortly before the pilot ran out of funding, taking a new job with CISCO's product security and incident response team. When members met a week later in Amsterdam for a post-mortem of sorts, they agreed that while the EuroCERT had benefits, the broader community was not ready to commit to a permanent centralizing organization. As the Amsterdam report noted:

> "In general, the responses to the pilot service have been positive and many have expressed their appreciation for the work done and the experiences gained during the past 2.5 years.

[13] Sergei Boeke, "National Cyber Crisis Management: Different European Approaches," *Governance* 31 (2018): 452.

[14] Rebecca Slayton and Brian Clarke, "Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989-2005," *Technology and Culture* 61, no. 1 (January 2020): 180. Robert Morris later became the first person charged under the new US Computer Fraud and Abuse Act (CFAA), signaling the start of a new era in computer crime prosecution.

[15] Slayton and Clarke, 180.

[16] "Software Engineering Institute - About the SEI," Carnegie Mellon University, 2023, https://www.sei.cmu.edu/about/index.cfm.

[17] Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (Cyber Conflict Studies Association, 2013).

[18] Slayton and Clarke, "Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989-2005," January 2020, 181.

[19] Slayton and Clarke, 182.

[20] Slayton and Clarke, 183.

[21] Slayton and Clarke, 186.

[22] Slayton and Clarke, 190.

[23] Slayton and Clarke, 190.

> Nevertheless, it has become clear that it will not be possible to establish a permanent operational European CERT co-ordination service to follow from the SIRCE pilot phase. This is mainly because the needs of the various networks in Europe and their CERTs are so different that it is not possible to reach consensus on the definition of a single permanent service."[24]

Many participants in the EuroCERT pilot agreed that the European CERTs should be empowered to "undertake operational services collaboratively," and in the long-term the community should strengthen its incident coordination processes.[25] However, pilot participants were unsure how to build a trusted broker across the community. Delegates disagreed on whether a "web of trust" was best housed in a single CERT, in regional CERTs, or in some other form of consortium.

Across Europe and the United States, computer security specialists recognized that CERTs benefited from building connections with each other to share information and incident management expertise. Yet, growth also caused a degree of anxiety, as previously close-knit communities struggled to maintain trust as they expanded. Even FIRST struggled with whether to open itself up to a broader array of incident response teams. In a report issued by the Future of FIRST Task Force in 1997, delegates noted "FIRST started as a small group of incident response teams, which developed a very 'trusted' relationship among themselves. The Task Force recognizes that such 'trust' is an important feature of the current FIRST environment."[26] The report goes on to state:

> "In its future vision for FIRST, the Task Force envisages a relatively open organization, reaching out to the entire IRST [Incident Response and Security Teams] community and facilitating cooperation, assistance and information exchange throughout that entire community. Handling and maintaining 'trust' among IRSTs [Incident Response and Security Teams] as FIRST evolves into this larger, more open organization will be a major challenge – which the Task Force has identified, which it believes can be surmounted, but for which it has not provided any concrete plan of attack."[27]

Ultimately, FIRST concluded that an open community was a necessity since incidents rarely affected one single CERT or CSIRT. FIRST also worried that without an inclusive model of growth, rival organizations could form, degrading the utility of the FIRST network and reducing its legitimacy. The organization struggled to identify ways to maintain trust as it expanded. FIRST committed itself to creating mechanisms for interaction across teams, including conferences and technical colloquia. Some degree of splintering, however, seemed inevitable, as incident response teams would "probably develop a small circle of IRSTs that are 'close friends,' and a still larger set that are 'relative strangers.'"[28] Such a development would "inevitably reduce the overall level of information sharing between IRSTs and the degree of teamwork and cooperation with which the entire incident response and security community responds to security incidents."[29]

The early experience of FIRST provides a useful framework for understanding later struggles faced by NATO and the EU in developing and centralizing crisis management structures for cyber incident response. The EU did not mandate centralized CSIRTs at the member state level until the 2016 Directive on Security of Network and Information Systems (the NIS Directive).[30] The Directive established a network of national CSIRTs, which could operate in response to a member state request in "discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Member State."[31] This began to lay the groundwork for more concerted cooperation in information-sharing and crisis management across the European Union. However, many EU member states still have far to go before achieving functional CERTs and crisis management structures.

---

[24] "Minutes of the Meeting to Discuss Future Collaborative Activities Between CERTs in Europe" (Amsterdam, The Netherlands, September 24, 1999), 1–2, https://tf-csirt.org/wp-content/uploads/2021/03/planningmeeting-1.pdf.

[25] "Minutes of the Meeting to Discuss Future Collaborative Activities Between CERTs in Europe," 3.

[26] "A Progress Report on the Findings of the Future of FIRST Task Force" (Santa Clara, California: Future of FIRST Task Force, April 1997), http://web.archive.org/web/19971108090929/http://www.first.org:80/docs/tf97/REPORT.txt.

[27] "A Progress Report on the Findings of the Future of FIRST Task Force."

[28] "A Progress Report on the Findings of the Future of FIRST Task Force."

[29] "A Progress Report on the Findings of the Future of FIRST Task Force."

[30] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union" (2016), arts. 31, 34, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=en. Article 34 states: "Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate network and information system incidents and risks. Member States should therefore ensure that they have well-functioning CSIRTs, also known as computer emergency response teams ('CERTs'), complying with essential requirements to guarantee effective and compatible capabilities to deal with incidents and risks and ensure efficient cooperation at Union level. In order for all types of operators of essential services and digital service providers to benefit from such capabilities and cooperation, Member States should ensure that all types are covered by a designated CSIRT. Given the importance of international cooperation on cybersecurity, CSIRTs should be able to participate in international cooperation networks in addition to the CSIRTs network established by this Directive."

[31] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, art. 12.

Multinational institutions face many potential tradeoffs when designing crisis response organizations. As Sergei Boeke has argued, "while a common assumption, the further centralization of decision making is not necessarily the most effective way of addressing a crisis, with network or decentralized authorities often more capable of judging which response would work best."[32] Centralization can help remove redundancies, but it can also create myopic or singular perspectives that hinder creativity.

Governing networks is a particularly complex challenge. Networks are "groups of three or more legally autonomous organizations that work together to achieve not only their own goals but also a collective goal."[33] Provan and Kenis identify three different types of network governance.

The first is participant-governed networks, which establish shared governance across network members. These networks are characterized by equality across members and high levels of trust within the network. Participant-governed networks "depend exclusively on the involvement and commitment of all, or a significant subset of the organizations that comprise the network."[34] This type of governance structure has a range of potential manifestations, from an extremely dense set of networked interactions whereby each institution interacts with every other organization to achieve shared governance, to more loosely knit forms of sharing arrangements.[35] Several countries have opted for this form of governance in cyberspace, including The Netherlands. The Dutch have a National Cyber Security Centre that functions as a centralized coordinating body and facilitator rather than top-down governor.[36]

The second form of network governance is lead organization-governed networks. These networks are centralized and hierarchical, with a lead agency responsible for coordinating activities and decisions across member organizations. In lead organization-governed networks, "all major network-level activities and key decisions are coordinated through and by a single participating member, acting as a lead organization. Thus, network governance becomes highly centralized and brokered, with asymmetrical power."[37] Denmark is one country that has adopted this approach in cybersecurity, designating its Center for Cyber Security as the institutional lead. Here, the Centre has become "*the* hub of government cyber capacity, monitoring networks and regulating standards, enforcing them when necessary. It functions as a first responder in times of crises, addressing incidents when APTs [Advanced Persistent Threats] have been detected but also in instances when high-level IT knowledge is required."[38]

Finally, the third form of network governance is network administered organizations (NAO). Here, the NAO functions as a separate and external entity which operates specifically to govern network activities.[39] Both Estonia and Czechia have adopted NAO models, whereby one institution operates as the hub of facilitation and centralized node of operations, coordinating expertise which is spread across several discrete agencies. The Estonians have set up a specific Information System Authority (RIA) to fulfil the role of NAO.[40] In Czechia, cyber incident response has been folded into the National Security Authority, which has a broader mandate to protect classified information in the country.[41]

There are many ways to assess the capacity of networked crisis response mechanisms. Boeke identifies three: (1) the capacity to make sense of a crisis; (2) the capacity to coordinate resources for response; and (3) the legitimacy of the response apparatus.[42] The three forms of network governance outlined above have distinct advantages and disadvantages. Participant-governed networks can be more easily legitimated because they involve the explicit and continual buy-in from network members. NAOs, meanwhile, can struggle to maintain legitimacy because the centralizing force has been created specifically for the purpose of governing the proposed network; thus, NAOs cannot fall back on other forms of legitimation, but must continually prove their worth as coordinating bodies. Lead organization-governed networks fall somewhere in between, depending on the particular profile of the central institution and the buy-in of other network members. Meanwhile, participant-governed networks often struggle to make sense of crises and coordinate responses. Actions taken by the network must be

[32] Sergei Boeke, "National Cyber Crisis Management: Different European Approaches," *Governance* 31 (2018): 450.

[33] Keith G. Provan and Patrick Kenis, "Modes of Network Governance: Structure, Management, and Effectiveness," *Journal of Public Administration Research and Theory* 18 (2008): 230.

[34] Provan and Kenis, 234.

[35] Provan and Kenis, 233–34.

[36] Boeke, "National Cyber Crisis Management: Different European Approaches," 454.

[37] Provan and Kenis, "Modes of Network Governance: Structure, Management, and Effectiveness," 235.

[38] Boeke, "National Cyber Crisis Management: Different European Approaches," 455.

[39] Provan and Kenis, "Modes of Network Governance: Structure, Management, and Effectiveness," 235.

[40] Boeke, "National Cyber Crisis Management: Different European Approaches," 457.

[41] Boeke, 458.

[42] Arjen Boin, Madalina Busuioc, and Martijn Groenleer, "Building European Union Capacity to Manage Transboundary Crises: Network or Lead-Agency Model?," *Regulation & Governance* 8 (2014): 418–36.

approved by constituent members, which can be lengthy and inefficient. Lead organization-governed networks can be more effective at marshalling resources because they have clearly designated cooperative functions ahead of the onset of crises.

Both the EU and NATO have created networks of cyber defense response mechanisms, instituting training exercises and cooperative burden-sharing structures.[43] However, the two institutions have enacted different network governance models. The EU has constructed a version of an NAO, whereby the Lithuanian MoD operates as the coordinating body that facilitates the PESCO project on Cyber Rapid Response Teams and Mutual Assistance in Cyber Security. While EU member states are free to join individual projects within the EU's Permanent Structured Cooperation (PESCO), they maintain a degree of independence in their commitment of resources and expertise. NATO, however, has opted for a participant-governed model. Allies maintain a high degree of autonomy even within the alliance's Cyber Rapid Reaction Team model. The decision to commit RRT resources is made directly by the North Atlantic Council, thus requiring the buy-in of all members states, i.e., all members of the network. NATO "serves as a platform for Allies to consult on cyber defence issues, share information on cyber threats, exchange best practice, and coordinate activities."[44] These two forms of network governance have advantages and disadvantages, which will be explored more fully in sections three and four.

The flexibility of the NAO structure has allowed the EU's CRRT project to shift its goals overtime, adapting from a purely reactive force to a proactive one that can be deployed to countries *before* they experience a crisis. While the CRRT maintains its crisis-first orientation on paper, in practice the teams have been most successful in fostering long-term goodwill with EU partner countries. In both Moldova and Mozambique, CRRTs were deployed to launch vulnerability assessments and help the countries develop stronger cyber defense postures. The CRRTs fit into broader EU projects in both countries – in Moldova, an expanded EU Partnership Mission in the country (EUPM Moldova), and in Mozambique, a broader EU training mission (EUTM-Moz).[45]

Yet, when a CRRT was readied for deployment to a country experiencing a crisis (Ukraine), the team was unable to get off the ground in time. These recent cases illustrate some of the drawbacks and benefits of an NAO-structured response mechanism.

NATO's RRTs, meanwhile, have never been initiated to deal with an ongoing crisis. The consensus-driven nature of the participant-governed structure has meant that any deployment of an RRT would need to be sanctioned by the entire North Atlantic Council (NAC), a time-consuming and formal bureaucratic process that has yet to be mobilized in response to a state request for cyber assistance.[46] NATO operates almost entirely through consensus mechanisms; it is unrealistic to believe that an RRT capability would be structured differently. Yet, there are benefits to this formalism. While no RRT has been used in response to a crisis, individual NATO countries have taken action to aid allies and partners. Crisis management is happening within the NATO alliance, just not through a centralized RRT capability.

[43] Boeke, "National Cyber Crisis Management: Different European Approaches," 460.

[44] "NATO Cyber Defence," Factsheet (NATO, April 2021), https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-fact-sheet-cyber-defence-en.pdf.

[45] "Key Trends and Statistics of the National Cyber Security Status of Lithuania 2022" (Lithuania: Ministry of National Defence, Republic of Lithuania and Cybersecurity National Coordination Centre, Lithuania, 2022), 5, https://kam.lt/wp-content/uploads/2023/06/KEY-TRENDS-AND-STATISTICS-OF-THE-NATIONAL-CYBER-SECURITY-STATUS-2022.pdf; "EU Partnership Mission in the Republic of Moldova (EUPM)," Official EU Website, EEAS, 2023, https://www.eeas.europa.eu/eupm-moldova_en?s=410318.

[46] Senior NATO Official, Author Interview on NATO Cyber Rapid Response Teams.

3 EU Cyber Rapid Response Teams

3.1 History

In 2017, Lithuania proposed the creation of the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT) as a new Permanent Structured Cooperation (PESCO) project. PESCO had been in the making for more than a decade. In 2007, the EU enacted the Lisbon Treaty, which amended the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), to establish the basis for the PESCO arrangement. Article 42(6) of TEU states:

> "Those Member States whose military capabilities fulfil higher criteria and which have made more binding commitments to one another in this area with a view to the most demanding missions shall establish permanent structured cooperation within the Union framework."[47]

Under the Lisbon Treaty, States are required to notify the European Council and the High Representative of the Union for Foreign Affairs and Security Policy (HR) of their intention of joining a PESCO arrangement.[48]

In September 2017, the Commission also issued a recommendation on "coordinated response to large-scale cybersecurity incidents and crises."[49] In its annex, the recommendation included a Blueprint that defined a pathway for EU involvement in cybersecurity "crises." The Blueprint laid out two potential types of crises: an incident which causes "disruption too extensive for a concerned Member State to handle on its own" and an incident which affects "two or more Member States or EU institutions with such wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at Union political level."[50] Although this definition still leaves much to be defined, the Blueprint provided a new mechanism for coordinating responses to cyber incidents across the EU. The Blueprint noted that "coordination at Union political level of the response shall be carried out by the Council, using the Integrated Political Crisis Response (IPCR) arrangements."[51] This constituted an important elevation of cyber incidents to the highest levels of EU governance mechanisms.

Later that year in December, the EU Council issued a declaration listing 17 PESCO projects, including the Lithuanian-led "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security."[52] The official establishment came a few months later in March 2017, with a Council decision christening the CRRT as one of 17 PESCO projects.[53]

The CRRT system was thus born. The process to formalize and operationalize the CRRT took several more years. In February 2018, Lithuania hosted a kick-off meeting in Vilnius to welcome participating member states to the CRRT process. Member states signed declarations of intent to join the PESCO project at the Foreign Affairs Council meeting on 25 June in Luxembourg and at the Baltic Defense Ministers Committee Meeting on 24 November in Vilnius. In between these two meetings on 29 August, legal Points of Contact convened in Vilnius to begin discussions of CRRT procedures and structures.

In October 2018, the CRRT system was tested at the Cyber Shield / Amber Mist exercises. These were the first common cyber tabletop exercises of their kind. Here, the CRRT model was stress-tested, and several additional organizational and logistical features were ironed out. On 15 January 2019, the Lithuanian PESCO project team published a legal memo for CRRT operations in Vilnius, which outlined the basis for CRRT legitimacy and integrated lessons learned from the 2018 exercises.

---

[47] European Union, "Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union," OJ C 202 § (2016), art. 42(6), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016ME%2FTXT.

[48] European Union, art. 46.

[49] "Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises," OJ L 239 § (2017).

[50] European Commission, "ANNEX to the Commission Recommendation (EU) 2017/1584 of 13 September 2017 on Coordinated Response to Large-Sclae Cybersecurity Incidents and Crises," OJ L 239 § (2017), https://eur-lex.europa.eu/eli/reco/2017/1584/oj.

[51] European Commission.

[52] "Defence Cooperation: Council Establishes Permanent Structured Cooperation (PESCO), with 25 Member States Participating," Press Release, European Council and Council of the European Union, December 11, 2017, https://www.consilium.europa.eu/en/press/press-releases/2017/12/11/defence-cooperation-pesco-25-member-states-participating/.

[53] EU Council, "Council Decision (CFSP) 2018/340 of 6 March 2018 Establishing the List of Projects to Be Developed under PESCO," (CFSP) 2018/340 § (2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018D0340.

3.2 Structure

The CRRT are built to bring together both military and civilian organizations. Lithuania is the lead country for this PESCO project. Seven additional countries participate: Belgium, Croatia, Estonia, the Netherlands, Poland, Romania, and Slovenia. The participant count is still growing. In late 2022, Belgium initiated proceedings to become a full participant.[54] Slovenia also expressed interest in transitioning to an active participant. In March 2023, both countries became official participating members.[55]

Five countries have joined as observers: Finland, France, Greece, Italy, and Spain. Czechia and Denmark have started negotiations to join the PESCO project in some capacity.[56]

Participants	Observers
Lithuania+	Czechia**
Belgium	Denmark**
Croatia	Finland*
Estonia	France*
The Netherlands	*Germany*
Poland	Greece
Romania	Italy
Slovenia	Spain

+ = lead country

* = previous participant country

** = prospective observer countries

NB: Germany has left the project

Participating member states form a council which serves as the primary decision-making body of the CRRT. This council is composed of the national points of contact (POCs) of the participating states. POCs are intended to be permanent designations, representing each participating state's respective national institution that interfaces with the CRRT. These POCs are also specifically to be pulled from "the political domain."[57]

Leadership of the CRRT rotates. Participating countries can each volunteer to serve as "Rotating Participant" (RP), a function that they hold for one calendar year (starting in January) after a unanimous decision from other participating countries. In recent years, however, the calendar year requirement has been somewhat relaxed, with states taking over the leadership role sometime in the spring. The RP is responsible for certain "necessary contributions," including the operational aspects of any CRRT. The RP also serves as one of the co-chairs of the CRRT Council. Lithuania maintains its designation as the lead country on the project every year, serving as the other co-chair of the CRRT Council along with several managerial duties.

Year	Leadership
2019	The Netherlands
2020	Lithuania
2021	Poland
2022	Romania
2023	Croatia

The CRRT Council sets the priorities for the CRRT and is responsible for any decisions to activate the CRRT in answer to a member state request for assistance. The Council also designates a Mission Coordinator who serves as the main technical point of contact for the CRRT. The Mission Coordinator is responsible for assembling a team in response to a member state Request and the subsequent council decision to active the CRRT.[58]

Importantly, each member state must designate a "national institution in the field of cyber security" to be responsible for requesting and facilitating CRRT assistance.[59] CRRT can only act in a member state's jurisdiction under the mandate of this national institution. The choice of institution is exclusively up to each participating member state. However, the idea behind the designation is for each member state to select an organization that has "the highest authority in the country in the field of cyber security" and is therefore able "to act on behalf of the State."[60]

[54] A. Cemerka, "Ministry of National Defence Preparing Plans for CRRTs to Assist Moldova," *Ministry of National Defence Republic of Lithuania*, September 29, 2022, Online edition, https://kam.lt/en/ministry-of-national-defence-preparing-plans-for-crrts-to-assist-moldova/.

[55] "Lithuanian-Coordinated EU Cyber Rapid Response Teams - Incident Response with the EU and in Support of EU Partners and Military Missions."

[56] Cemerka, "Ministry of National Defence Preparing Plans for CRRTs to Assist Moldova."

[57] Egle Vasiliauskaite and Tadas Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security, Key Roles and Procedures for the CRRTs' Operations, Lessons Learnt from the Cyber Shield / Amber Mist 2018 Exercise," 2019, 11.

[58] Vasiliauskaite and Sakunas, 11.

[59] Vasiliauskaite and Sakunas, 12.

[60] Vasiliauskaite and Sakunas, 12.

Annex 1 - PESCO CRRT incident report

Requesting Entity	Country	Lithuania
	Organisation	National Cyber Security Centre (NCSC) under the Ministry of National Defence
Date of Request	11-10-2018	
Primary Mission Point of Contact	Name and Surname	
	Position	
	Organisation	NCSC under the Ministry of National Defence
	Telephone number	
	Email Address NU/NS/Internet	
Alternative Mission Point of Contact	Name and Surname	
	Position	
	Organisation	NCSC under the Ministry of National Defence
	Telephone number	
	Email Address NU/NS/Internet	
Incident evaluation	Affected entities	LTU transport, BT Energy, BT Ministry of Transport and Communications
	Affected sectors	Transportation, Energy, Government
	Incident duration	08-10-2018/Ongoing
	Incident source	Possibly the endpoint device in "LTU transport"
	Characteristics	"LTU transport" administration network has been encrypted as well as some parts of the OT network. Incident has affected other entities, such as BT Energy, BT Ministry of Transport and Communications. NCSC has been informed about other ongoing cyber-attacks (DDoS, defacement, and data exfiltration) in BT Energy, BT Ministry of Transport and Communications and other critical entities.
	Possible outcomes (nationally and internationally)	Disruption of critical services: unable to deliver cargo, power blockouts in some parts of Lithuania and Latvia.
	Possible scale (nationally and internationally)	Considering cargo delivery – Baltic Sea region; Considering power provision – Baltic States and (possibly) Crimsonia.
Expectations of RRT Assistance (from the point of view of the Requesting Entity):	Mission Objectives (high-level)	Investigate ransomware source, stop its spreading, restore critical services within transport, energy, government sectors.
	Desired Assistance (area of focus, priorities for each area)	Forensic investigation (LTU transport, BT Energy), network analysis and critical services backup (LTU transport, BT Energy ICS network).
	Criteria for Success or Termination	Restored critical services.
	Anticipated Duration of the Mission	2 days.
Requestor Details	Name	
	Position	
	Organisation	NCSC under the Ministry of National Defence
	Telephone number	
	Email Address NU/NS/Internet	
Requestor Authority	NCSC under the Ministry of National Defence of Republic of Lithuania	

Figure 1: PESCO Incident Report Form

Hosting member states – the states that request and receive assistance – are also required to designate a technical point of contact which will interface directly with the CRRT Mission Coordinator. This role is structured to support the CRRT with in-depth knowledge of state infrastructure. The technical POC is also in charge of authorizing the actions of the CRRT if necessary. Host states are also asked to designate a logistics point of contact to take care of all practical questions regarding lodging, liability waivers, and other necessities.

3.2.1 CRRT Activation

In order to activate a CRRT, a member state is required to submit a request using the Incident Report form (figure 1). The form includes a brief incident evaluation of the expectations of CRRT assistance, as well as details of the key points of contact for the requesting organization and mission lead. Once the request is received, the co-chairs of the CRRT Council alert the POCs of all participating member states to the request for CRRT activation, forwarding the Incident Report Form to provide further information. Participating member states then agree on a decision-making timeline, which should be "a reasonable time for the Member States to assess the severity of the incident and legitimacy of the request to decide whether the CRRT should be activated and sent to the requesting Member State. It should also be short enough to prevent the overdue arrival of the CRRT at the Member State to manage the incident."[61] During the Cyber Shield / Amber Mist 2018 exercises, participating states agreed on a timeline of 24 hours.

If the Council were to decide to active the CRRT, then the Chairman of the Council would alert the mission coordinator. The mission coordinator would then be responsible for assembling a team of experts. The team would be selected based on the skill sets necessary for the incident at hand. The mission coordinator would work closely with the national POCs for technical and logistical issues to execute the mission.

3.2.2 CRRT Composition

The composition of a CRRT is a complex and delicate matter. The Lithuanian project management team suggested two potential composition strategies:

(1) A team could be "pre-composed" of participating member states, with each state designating a national expert with a "specific set of skills."[62]
(2) If option (1) is not possible, then the CRRT may be composed entirely of experts from the member state serving as the lead of the CRRT rotational system at the time of the incident. The final team would then be composed by the mission coordinator who would make his selection based on the skills required to respond to the specific incident.[63]

The Lithuanian team also assembled an ideal template for the profiles of CRRT members:

Mission Coordinator	1 person
Malware / Forensics	1-2 people
Network Forensics	1 person
Network General Monitoring	1 person
Infrastructure / Network	1-2 people
Logistics Coordinator	1 person
Exercise Coordinator	1 person

The target team size was originally identified as six specialists – four experts, one mission coordinator, and one logistics coordinator.

In the 2018 exercises, the Netherlands was as the lead member state during the exercise. The Dutch delegate served as both the mission coordinator and logistics coordinator. Four other experts were required: a network forensics specialist, an IDS monitoring specialist, a malware specialist, and an ICS specialist for the specific manufacturer involved in the incident.[64] These were provided by Estonia, Poland, Romania, and Finland.[65] Later, however, the ideal team size was expanded to 8-12 experts delegated by the participating member states.[66]

The Lithuanian project team also proposed that each member of the CRRT must have an existing security clearance to manage "all potential risks in relation to the access to sensitive information/critical infrastructure during the mission."[67]

The CRRT is funded by both the lead member state and the hosting state.[68] The lead member state is responsible for covering travel and other costs prior to the arrival of the CRRT in the host state. The host state is subsequently responsible for accommodations of the CRRT, airport check-ins, transportation within the country, and other costs incurred once the CRRT has arrived on its soil.

Once the CRRT arrives in the host state, participants are expected to sign liability waivers and non-disclosure agreements.[69]

[61] Vasiliauskaite and Sakunas, 18.
[62] Vasiliauskaite and Sakunas, 23.
[63] Vasiliauskaite and Sakunas, 23.
[64] Vasiliauskaite and Sakunas, 24.
[65] Vasiliauskaite and Sakunas, 24.
[66] "EU Cyber Rapid Response Teams to Support Ukraine."
[67] Vasiliauskaite and Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Political Memo," 24.
[68] Vasiliauskaite and Sakunas, 27.
[69] Vasiliauskaite and Sakunas, 27.

3.3 CRRT Purpose

The Lithuanian-led PESCO project has been explicit about its primary goals. First, the project is built to bring together military and civilian organizations to enhance cooperation in security. The Lithuanian project team argued that "we have made a conclusion that the origin of a person (nationality, civil/military background) is not as important as the mandate of the mission, which will be the factor uniting different members in one team."[70]

The CRRT project endeavors to develop its own technical toolkit to defend and remediate cyberattacks, as proposed by the Lithuanian National Cyber Security Centre. Here, the benefits of the program include building shared cyber expertise and utilizing a common capability for remediation and response. Overall, the CRRT is intended to enhance EU institutional and member state resilience. The Lithuanian Delegation called the project "the missing puzzle piece to complement the existing cyber security mechanisms."[71]

Lithuania outlined four key priority areas for the project, in order of their significance:

(1) Supporting affected participating member states.
(2) Supporting other EU member states that are not members of the PESCO project.
(3) Supporting EU institutions.
(4) Supporting CSDP Missions.
Supporting Partner countries (long-term).

Each goal has a different prospective timeline, with goals one, two, and three as short and medium-term objectives for the project. Goals four and five have longer time horizons, intended to be addressed once member states have provided each other with necessary support. The CRRTs have several intended use cases which align with the priorities of the project.

3.4 Use Cases & Legal Rationales

3.4.1 EU Mechanisms for CRRT Authorization

There are two primary EU mechanisms that allowed for CRRT deployment. The first is the Mutual Assistance Clause, which is stipulated in Article 42 of the Treaty on European Union (TEU):

> "If a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power, in accordance with Article 51 of the United Nations Charter. This shall not prejudice the specific character of the security and defence policy of certain Member States. Commitments and cooperation in this area shall be consistent with commitments under the North Atlantic Treaty Organisation, which, for those States which are members of it, remains the foundation of their collective defence and the forum for its implementation."[72]

Importantly, the EU has moved towards defining armed aggression to be inclusive of cyberattacks that reach a certain threshold.[73] When instigating the Mutual Assistance Clause, it "is about impact rather than the choice of a weapon."[74]

When a member state chooses to trigger the Mutual Assistance clause, the request goes directly to other member states for bilateral support rather than initiating an EU institutional process. Thus, the CRRT could be used if a member state request for aid requires a cyber supporting element. The CRRT constitutes a possible joint capability which could be marshalled to answer the request for assistance.[75] The use of the clause requires certain reporting mechanisms as well: states need to alert the UN Security Council to any use of the clause.[76]

[70] Vasiliauskaite and Sakunas, 25.

[71] Lithuanian Delegation, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security" (Council of the European Union General Secretariat, Brussels, Belgium, March 6, 2019).

[72] European Union, Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, art. 42(7).

[73] "Article 42(7) TEU - The EU's Mutual Assistance Clause," EEAS, October 6, 2022, https://www.eeas.europa.eu/eeas/article-427-teu-eus-mutual-assistance-clause_en.

[74] Egle Vasiliauskaite and Tadas Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security, Legal Basis for the CRRTs' Operations" (Vilnius, Lithuania: Ministry of National Defence of the Republic of Lithuania, January 15, 2019), 17.

[75] Vasiliauskaite and Sakunas, 18.

[76] "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security Legal Basis for the CRRTs' Operations," 18; Jochen Rehrl, "Invoking the EU's Mutual Assistance Clause. What It Says, What It Means.," *EGMONT Royal Institute for International Relations* (blog), November 20, 2015, https://www.egmontinstitute.be/invoking-the-eus-mutual-assistance-clause-what-it-says-what-it-means/.

The second EU mechanism is the Solidarity Clause, which is outlined in article 222 of the Treaty on the Functioning of the European Union (TFEU):

> "The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster."[77]

Here, a cyberattack could constitute either a terrorist threat/attack or a man-made disaster, depending on the particular aggressor. In order for the Solidarity Clause to be invoked, the "political authorities of the affected Member State shall address their invocation to the Presidency of the Council as well as to the President of the European Commission through the Emergency Response Coordination Centre."[78]

3.4.2 Blueprint Use Cases

The Lithuanian delegation has been careful to denote the distinction between CRRT employment in proper cybersecurity "crises" as defined by the 2016 Blueprint versus use cases in incidents that fall under this threshold.

In incidents that rise to the level of a "crisis," the Blueprint is invoked. The Blueprint is outlined in the Annex to the Commission recommendation on "coordinated response to large-scale cybersecurity incidents and crises," which was issued in September 2017.[79] Here, CRRT can be identified as a capability to use in a solution to such a crisis. The Blueprint defines a crisis as one of two qualifying incidents:

(1) An incident where the disruption is too large or extensive for a member state to respond single-handedly.[80]
(2) Incident affecting two or more member states / EU institutions "with such a wide-ranging and significant impact that they require policy coordination & response at the Union's level".[81]

The definition here is not particularly specific, raising questions about how the Union defines a "significant" or "wide-ranging" impact in the environment of cyberspace. However, as mentioned in 3.1, the Blueprint does provide a new mechanism for addressing cyberattacks at the highest levels of European Union institutions. Here, the Blueprint is implemented by the European Council using the Integrated Political Crisis Response (IPCR) rules. In this scenario, the Commission and HR would identify all relevant EU instruments, including military assets, which could be used to respond to a cyber crisis.

The Lithuanian project team has argued that in either case of Blueprint activation, a CRRT could be used to support a Union response to a cyber crisis. The CRRT are an important potential mechanism of response that could be easily mobilized through the IPCR process. The team notes that the CRRTs are not redundant; rather, they reinforce and reflect the Blueprint's guiding principles of proportionality, subsidiarity, and complementarity as "the CRRTs equip the Member States, which have the primary responsibility for the response in case of large-scale cybersecurity incidents affecting them at the same time enhancing the interaction and cooperation with the existing mechanisms in the field."[82]

3.4.3 Non-Blueprint Use Cases

In incidents below the threshold of a cybersecurity "crisis," member states could very clearly invoke CRRT support. In fact, this is the most likely use case.

The Lithuanian project team has outlined CRRT activation processes for several priority areas of the PESCO project.

The first priority of the PESCO project is to offer support to affected EU member states that have joined the project. The legal basis for CRRT activation rests on member states sovereignty. Each participating member state is "entitled" to ask for assistance with any organization in accordance with their state sovereignty. Therefore, "state invitation" is a sufficient legal basis for CRRT to operate in member state territory.[83] Importantly, the member state must identify a national institution that can request the CRRT with authority from its own state government. Thus, once it enters member state territory, the CRRT can only operate "within the mandate of the national institution (most likely national CERT), which requested support of the CRRT."[84]

---

[77] European Union, Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, art. 188 R (1).

[78] Vasiliauskaite and Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Legal Memo," January 15, 2019, 20.

[79] European Commission, ANNEX to the Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-sclae cybersecurity incidents and crises.

[80] European Commission.

[81] Lithuanian Delegation, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security."

[82] Vasiliauskaite and Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Legal Memo," January 15, 2019, 23.

[83] Lithuanian Delegation, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security."

[84] Lithuanian Delegation.

Supporting other EU member states that are not actively participating in the PESCO project is the second priority area outlined by the Lithuanian team. Here, the same principles of state sovereignty provide the basis for legitimation: an EU member state can request assistance from any entity. The PESCO Council must then decide whether to respond to the request for support and issue a decision in a timely manner.

The third priority area for the CRRT project is to support EU institutions and organizations. The legal authority for CRRT activation is somewhat more complicated than in the previous two priority areas. EU institutions do not have the same sovereign authority as member states to designate one (national) institution to act on its behalf, Instead, each EU entity "has autonomy and is a separate decision-maker. In the case of a cyberattack/cyber incident, an EU institution remains the owner of the incident. For this reason, the consent/invitation of a certain EU institution would be necessary for the CRRTs to be able to operate in its assistance."[85]

In this use case, CERT-EU has an important role to play. CERT-EU is the EU's hub for cybersecurity information exchange and incident response coordination affecting EU institutions, bodies, and agencies. The Lithuanian project team envisioned that CERT-EU would coordinate with the CRRT in a cooperative model: "Instead of acting separately, CRRTs could support the EU institutions, agencies and bodies upon the request of CERT-EU with the consent of the affected EU institution/ agency/ body."[86] An activated CRRT would thus support CERT-EU within its operational mandate.[87]

The fourth priority area involves supporting EU CSDP missions. These missions are managed by the European External Action Service (EEAS), which reports to the High Representative for Foreign Affairs and Security Policy (HR). Here, the mandate of the CSDP mission provides the legal basis. The cyber element of support provided by the CRRT could be included in the overall mission. The CRRT could also be activated if the mission itself was the target of a cyberattack and needed support. In this case, no mandate would be required. Instead, "it is sufficient for the Operation/ Force Commander to include the required cyber capability (the CRRTs) in Force Generation Process."[88]

The fifth and final priority of the PESCO project is to support non-EU Partner countries, including Norway, the UK, Ukraine, Moldova, and Georgia. As outlined earlier, this is the longer-term goal of the project. Here, as with earlier priority areas, state requests for assistance provide the main legal basis for action. The Lithuanian project team notes that in this use case, treaties are not necessarily required to allow for CRRT activation. The CRRT process could be arranged through multilateral agreements instead.[89] Partner countries requesting assistance would need to designate a national institution to receive the CRRT; as with other use cases, the CRRT would thus operate under the mandate of the institution. Importantly, participating PESCO project countries would need to decide through the CRRT Council whether to support the partner country's request.[90] Resource constraints could make such support more difficult. Additionally, as this is a longer-term goal of the project, the CRRT Council might instead choose to prioritize short- and medium-term goals in the foreseeable future.

3.4.4 Preventative Activity & Standing Capacity

Although many of the CRRT use cases involve activating teams in direct response to an unfolding crisis, the PESCO project also has mechanisms for being deployed proactively. Preventative actions, including vulnerability assessments and election monitoring, are potential use cases for the arrangement.[91] The Lithuanian project team notes that these types of CRRT activations can be planned for by the member states ahead of time, making them an attractive possible use case. The team notes that requests for such types of activities, however, should be processed through a separate procedure than the Incident Response Form used for crisis management scenarios.

Although this use case was the lowest priority at the outset of the CRRT project, preventative missions have become the clearest successes of the teams. The CRRT deployment to Mozambique also created a new use case – a standing capability. In mid-2023, the Lithuanian Ministry of Defense announced:

> "Following the completion of the mission in Mozambique this March, the Lithuanian-

[85] Vasiliauskaite and Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Legal Memo," January 15, 2019, 12.

[86] Egle Vasiliauskaite and Tadas Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security, Legal Basis for the CRRTs' Operations" (Vilnius, Lithuania: Ministry of National Defence of the Republic of Lithuania, January 15, 2019), 12.

[87] Vasiliauskaite and Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Legal Memo," January 15, 2019, 12.

[88] Vasiliauskaite and Sakunas, 14.

[89] Vasiliauskaite and Sakunas, 15.

[90] Vasiliauskaite and Sakunas, 15.

[91] Vasiliauskaite and Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Political Memo," 29.

> coordinated European Union Cyber Rapid Response Teams (CRRT) can be used as a standing capability for internal EU needs as well as in support of EU partners and the EU Common Security and Defence Policy missions and operations."[92]

Indeed, the CRRT project has been expanding its preventative mission. Lithuania has also been working through its Ministry of National Defense on CYBER4DE, a project to develop a multifunctional cyber rapid response toolbox. CYBER4DE "stems directly from the needs of the Cyber Rapid Response Teams (CRRTs)" and "aims to enhance the processes and practices of CRRTs for a faster uptake of the new tools and increased effectiveness in the operating domain in different complex national and international scenarios."[93]

The country has partnered with organizations from seven other EU member states to develop the toolbox, with the goal of strengthening EU cyber defense capabilities. The project, which was launched in December 2021, is funded by the European Defence Industry Development Programme (EDIDP) and coordinated by Lithuania.[94] This is the first such type of project led by Lithuania. The overall grant is worth 9.3 million euros.

The project is supported by government partners as well as private sector actors from seven EU member states. The defense ministries of Estonia, France, Poland, and Romania support the Lithuanian-led project, while companies from Croatia, Estonia, France, Italy, Poland, Romania, and Lithuania are also participating in CYBER4DE.[95]

The toolbox concept is based on four modules: (1) workplace, (2) sensors, (3) back-office, and (4) cloud services. The toolbox is intended to be highly modular and flexible, providing specific functions to help manage common cybersecurity incidents and be integrated into existing solution sets.[96] The toolbox will be a major new addition to the CRRT PESCO project and will be "available for ensuring national readiness for an effective response to cyber incidents."[97] The toolbox will also be made available to other military and civilian institutions, although it is being engineered with the specific needs of the CRRT in mind. The toolbox is set to be completed by mid-2024, after extensive testing with the CRRT. In general, the toolbox capacity fits with the CRRT project's broadening objective of creating standing capacity and upgrading national and international cyber defense *before* an incident occurs.

3.4.5 Integration with CSIRTs Network

Under the 2016 NIS Directive, the European Union established a network of CSIRTs to facilitate and coordinate across national CERTs. According to the directive, this network is intended to operate "at the request of a representative of a Member State's CSIRT, discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Member State."[98]

The Lithuanian project team has argued that while the CSIRT network is an important tool for incident management, it functions quite differently from the CRRT project. The team defines identifying a coordinated response as a form of facilitation, involving information gathering and evidence collection. The CSIRT network is not intended to provide operational support and does not have a mechanism for delegating teams to travel to a member state in times of crisis. Therefore, the project team argues, "although both CSIRTs Network and the CRRTs operate in the field of cyber incident management, the specificity of their work significantly differs. The CRRTs would offer an operational capacity, which would be at Member States' disposal."[99]

---

[92] "Lithuanian-Coordinated EU Cyber Rapid Response Teams - Incident Response with the EU and in Support of EU Partners and Military Missions."

[93] "Lithuanian-Led EU Consortium Develops next-Generation Multifunctional Cyber Toolbox for Defence," *Ministry of National Defence Republic of Lithuania*, May 9, 2022, https://kam.lt/en/lithuanian-led-eu-consortium-develops-next-generation-multifunctional-cyber-toolbox-for-defence/.

[94] "Progress in Development of Multifunctional Cyber Rapid Response Toolbox at the Ministry of National Defence," *Ministry of National Defence Republic of Lithuania*, June 22, 2022, Online edition, https://kam.lt/en/progress-in-development-of-multifunctional-cyber-rapid-response-toolbox-discussed-at-the-ministry-of-national-defence/.

[95] "Lithuanian-Led EU Consortium Develops next-Generation Multifunctional Cyber Toolbox for Defence."

[96] "Lithuanian-Led EU Consortium Develops next-Generation Multifunctional Cyber Toolbox for Defence."

[97] "Progress in Development of Multifunctional Cyber Rapid Response Toolbox at the Ministry of National Defence."

[98] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, art. 12(3d); see also: Vasiliauskaite and Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Legal Memo," January 15, 2019.

[99] Vasiliauskaite and Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Legal Memo," January 15, 2019, 22.

3.5 Implementation Challenges

The CRRT project has issued a robust set of public procedures and operational guidelines for activation. However, several key implementation challenges remain.

One central challenge with the CRRT model has been identifying skill sets for team composition. The Cyber Shield / Amber Mist 2018 exercise raised questions about how well participating state representatives understood the value add of their cyber capabilities:

> "During the table top exercise, the Mission Coordinator addressed the participating Member States in the Council asking what skills which State could offer (option No. 1 for the composition of the team). This part was necessary to test the knowledge of the delegates of the Member States regarding the national expertise each country could share in the time of need. The process was simulated, however, the exercise showed that the representatives did not have knowledge of their national capabilities. Such knowledge will be vital in the next exercise and should be ensured by the Member States."[100]

Given that CRRTs are intended to be small, agile teams that can deploy quickly, the lack of knowledge of national capabilities will likely significantly slow down the CRRT deployment process. The project goals of integrating civilian and military institutions across participating member states provides another possible complication, as coordination across so many institutions can severely slow down response timelines.

The Lithuanian project team has identified another possible composition strategy, which would involve sending only experts from one participating member state (the state currently chairing the project Council). However, this option does not achieve the same kind of integration of capabilities across states as a multinational team does. Although a team composed of a single member state's experts would be easier to deploy quickly, it does not capitalize on the spirit of the PESCO project. Yet, few EU countries have the specialized cyber capabilities to be mobilized on short notice.

Another challenge has been around liability and data sharing. The Lithuanian project team has argued for restricting CRRT membership to experts with existing security clearances, thus effectively limiting participation to government actors. Private sector involvement is therefore quite difficult, as most experts working at corporations will not have security clearances and thus will be unable to join a CRRT quickly. The Lithuanian team argued that the national security concerns needed to take precedence,[101] but this line of thinking neglects the very real fact that private sector companies are already on the first line of cyber incident response management.

Private sector expertise could be particularly important in response scenarios because many governments use off-the-shelf products for their government ICT infrastructure. In the 2018 exercises, the Mission Coordinator asked the participating state's technical POC about the operating system being used and its manufacturer. However, for the future, participating states agreed that the CRRT would not be responsible for contacting the manufacturer in the case of an actual cyber incident. Instead, this would be left to the hosting member state.[102] If the CRRTs will not be pulling experts from the private sector, however, this may make public-private cooperation and coordination more difficult to achieve.

A third challenge arises around the question of attribution. The 2018 exercises simulated a cyberattack perpetrated against Lithuania, where the country experienced a "'dangerous incident'" as defined by its National Cyber Incident Management Plan and requested a CRRT for support.[103] The exercise reinforced that attribution should not be the primary goal of the CRRT, although the team would endeavor to preserve any evidence uncovered during the support process in order to facilitate later investigations by relevant member state authorities.[104] The dedication to attribution-agnostic activity may not be shared across all EU member states, however. Other states may wish to make a public attribution, depending on the political situation that arises from the incident.

At the 2018 exercises, states also agreed to establish a "commonly agreed and nationally tailored threshold" for deciding when a member state should request activation of a CRRT. This articulation is rather ambiguous. How would one reconcile these two competing visions of a threshold? Participating states might have very different levels of cyber security competency, meaning that an

[100] Vasiliauskaite and Sakunas, "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Political Memo," 23.

[101] Vasiliauskaite and Sakunas, 24.

[102] Vasiliauskaite and Sakunas, 21.

[103] Vasiliauskaite and Sakunas, 15.

[104] Vasiliauskaite and Sakunas, 18.

incident requiring CRRT assistance may look very different from one state to the next. Delegates agreed that member states should follow the NIS Directive recommendation to establish CRRT activation threshold.[105]

As section 5 will illustrate, the CRRTs have been most effective not in crisis response roles but in proactive vulnerability assessment missions. CRRTs seem to work best as a symbol of goodwill, helping to foster cooperation particularly between EU partner countries (Moldova and Mozambique). These types of missions do not face the same implementation challenges. The CRRTs have more time to assemble teams when they are working ahead of crises, and they can build coalitions and partnerships on the ground slowly and thoughtfully. Liability and data-sharing issues can be hashed out thoroughly ahead of time; the teams do not need to operate quickly to dispel an ongoing crisis, but rather can take their time to build resilience and capacity in the partner countries. The CRRTs have become a prominent public avenue for EU activity, but they often operate at the margins of much broader partnership efforts. In Moldova, the CRRT entered in conjunction with the larger EUPM-Moldova mission set; similarly, in Mozambique, the CRRT was simply one facet of a much broader EU training mission. CRRTs seem to work best when they are neither rapid nor responsive, but rather deliberate and proactive.

[105] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, paras. 27 & 28.

4 NATO Rapid Reaction Teams

4.1 History – The Rise of Cyberspace in NATO Policy

During the upheaval of the security environment in the wake of 9/11, cyberspace surfaced as part of the political agenda within NATO. At the 2002 Prague Summit, the North Atlantic Council mentioned cyberattacks as a new area for defensive focus, embedded in a broader declaration that focused on international terrorism as the preeminent threat faced by the alliance.[106] The NAC approved the implementation of a Cyber Defense Program later that year, which established a new NATO Computer Incident Response Capability (NCIRC).[107]

The following few years would see little policy evolution – instead, NATO's focus turned to Iraq. At the 2004 Summit in Istanbul, the word "cyber" did not appear once in any public statements or press releases.[108] Neither did "cyber" make an appearance at the 2005 Brussels Summit.[109] At the 2006 Summit in Riga, cyberspace made several brief appearances as an area where further NATO investment was needed. The North Atlantic Council committed to develop an information sharing capability to improve "protection of our key information systems against cyberattack" and endorsed Comprehensive Political Guidance which emphasized the need for further investment to mitigate cyber threats.[110]

The 2007 cyberattacks against Estonia mark a clear shift in Alliance thinking. In April and May of 2007, the government of Estonia faced an onslaught of cyberattacks after its decision to move the Bronze Soldier to a less central location in Tallinn. The statue, dedicated in 1947 by Soviet authorities to commemorate the Red Army liberation of Estonia from the Nazis, had long been a controversial emblem of tensions between ethnic Russians and Estonians.[111] The Baltic country is home to a small Russian-speaking minority – a population that was purposefully increased through relocation efforts by the Soviets throughout the Cold War.[112] Ethnic Russians generally saw the Bronze Soldier as a symbol of Soviet victory in WWII, while Estonians interpreted the statue as a reminder of the long Soviet occupation. The statue controversy reached a head in late April 2007 as the Estonian government prepared for its relocation. For about 22 days from 27 April to 18 May, the country experienced an onslaught of cyberattacks, including DDoS attacks targeting government websites, online banking systems, and media organizations.[113] Most attacks originated from Russian-language networks, although the Russian government has officially denied any involvement in the incident.[114]

The attacks raised cyber as a key emerging threat area, providing a tangible example of the kind of havoc that can be wreaked on government ICT systems. In the wake of the attacks, Estonia formally requested emergency assistance from the Alliance to defend its digital infrastructure. This was the first time a member state had asked for help specifically in cyberspace. NATO sent cyber experts to Estonia to help defend against the attacks.[115] In June 2007, member state defense ministers met and declared the need for "urgent work" on cyber defense, which instigated an internal review of the Alliance's own network infrastructure.[116]

NATO quickly began preparing its first cyber defense policy. In January 2008, the policy was approved by the

[106] "Prague Summit Declaration" (Prague, Czech Republic: North Atlantic Treaty Organization, November 21, 2002), https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

[107] "Defending against Cyber Attacks," 2014, https://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf.

[108] See, for example: "Istanbul Summit Communiqué" (Istanbul, Turkey: North Atlantic Treaty Organization, June 28, 2004), https://www.nato.int/docu/pr/2004/p04-096e.htm; "The Istanbul Declaration: Our Security in a New Era" (Istanbul, Turkey: North Atlantic Council, June 28, 2004), https://www.nato.int/docu/pr/2004/p04-097e.htm.

[109] "Statement Issued by the Heads of State and Government Participating in a Meeting of the North Atlantic Council in Brussels" (Brussels, Belgium: North Atlantic Council, February 22, 2005), https://www.nato.int/docu/pr/2005/p05-022e.htm.

[110] "Riga Summit Declaration" (Riga, Latvia: North Atlantic Council, November 29, 2006), https://www.nato.int/docu/pr/2006/p06-150e.htm; "Comprehensive Political Guidance" (Riga, Latvia: NATO, November 29, 2006), https://www.nato.int/cps/en/natolive/official_texts_56425.htm.

[111] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Studies* 4, no. 2 (Summer 2011): 49–60.

[112] Herzog.

[113] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective" (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008).

[114] James Pamment et al., "Hybrid Threats: 2007 Cyber Attacks on Estonia," Hybrid Threats: A Strategic Communications Perspective (Tallinn, Estonia: NATO Strategic Communications Centre of Excellence, June 6, 2019), https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

[115] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, https://www.wired.com/2007/08/ff-estonia/; "NATO Sees Recent Cyber Attacks on Estonia as Security Issue," *DW*, May 26, 2007, http://www.dw.com/en/ nato-sees-recent-cyber-attacks-on-estonia-as-security-issue/a-2558579.

[116] "NATO Summit Guide" (Warsaw, Poland: NATO, July 8, 2016), 127, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf.

allied defense ministers.[117] In April at the Bucharest Summit, the policy was publicly announced, albeit with little in the way of specifics. The Summit declaration noted that, "Our Policy on Cyber Defence emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon requests, to counter a cyber attack."[118] Interestingly, the Estonian attacks are not named explicitly in the summit declaration, although the NATO Secretary General Jaap de Hoop Scheffer did mention them in passing in a German Marshall Fund side-event keynote at the Summit.[119]

Only a few months later, the specter of cyberwarfare once against gained traction as the international armed conflict between Russia and Georgia erupted. NATO recognized that cyberattacks had the potential to "become a major component of conventional warfare."[120]

NATO soon began moving towards more concrete policy articulations and institution building. In the 2009 Strasbourg / Kehl Summit, the North Atlantic Council announced the creation of a Cyber Defence Management Authority, as well as the activation of the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia.[121] Cyber defense also became a key rationale behind the need for an updated NATO Strategic Concept. In a press conference at the Summit, NATO Spokesman James Appathurai argued that the concept needed to reflect the new world in which the Alliance operated, noting that "no where does it [the 1999 Strategic Concept] reflect the fact that NATO would now have, as it does now have, a cyber defence centre, a deployable cyber defence capability."[122]

By 2010, cyber defense had taken a leading role in NATO policy. At the Lisbon Summit, cyber was central: the Summit declaration promised that the NCIRC would be brought up to full operational capability by the end of the year, and that all NATO bodies would be brought under centralized cyber defense protection.[123] The Summit declaration also announced that a newly revised cyber defense policy would be launched by June 2011 – the second full NATO cyber policy. The new Strategic Concept was also launched. Although cyber only made two appearances in the document (once as a new threat domain, and once as an area where NATO needed to invest to achieve defensive and deterrent capabilities), this still denoted a marked shift in Alliance attention.[124]

After it was drafted and approved by the Alliance's Defense Ministers in June 2011, NATO launched its revised Cyber Policy. This policy called for the establishment of minimum cybersecurity requirements for all NATO Allies with national networks that connected or processed information from NATO. These thresholds would later evolve into the Cyber Defense Pledge and become a cornerstone of Allies' individual investment parameters. Importantly, the policy also included the first indication of how a cyberattack could fit into NATO's broader collective defense architecture. The policy factsheet noted that "any collective defense response is subject to decisions of the North Atlantic Council. NATO will maintain strategic ambiguity as well as flexibility on how to respond to different types of crises that include a cyber component."[125] Article 5 is not explicitly mentioned, but the Alliance was beginning to move toward a more robust understanding of how the Washington Treaty might apply to cyberspace.

The 2011 policy also began to outline what would become the Cyber Rapid Reaction Team:

> "NATO will provide coordinated assistance if an Ally or Allies are victims of a cyber attack. To facilitate this, NATO will enhance consultation mechanisms, early warning, situational awareness and information sharing among the Allies. To facilitate these activities, NATO has a framework of cyber defence Memoranda of Understanding [MOU] in place between Allies' national cyber defence authorities and the NATO Cyber Defence Management Board."[126]

The policy did not yet articulate a formal integrated response team at the NATO-level, but privately NATO was already thinking about a rapid reaction force structure for cyber defense. RRT capabilities had indeed been explored

[117] "NATO Summit Guide," 127.

[118] "Bucharest Summit Declaration" (Bucharest, Romania: North Atlantic Council, April 3, 2008), https://www.nato.int/cps/en/natolive/official_texts_8443.htm.

[119] Jaap de Hoop Scheffer, "Keynote Speech by NATO Secretary General" (Bucharest Conference, German Marshall Fund, Bucharest, Romania, April 2, 2008), https://www.nato.int/cps/en/natohq/opinions_7608.htm.

[120] "NATO Summit Guide," 127.

[121] "Strasbourg / Kehl Summit Declaration" (Strasborg, France / Kehl, Germany: North Atlantic Council, April 4, 2009), https://www.nato.int/cps/en/natolive/news_52837.htm.

[122] James Appathurai, "Press Briefing by NATO Spokesman" (NATO Summit meetings of Heads of State and Government, Kehl, Germany, April 3, 2009), https://www.nato.int/cps/en/natolive/opinions_52841.htm.

[123] "Lisbon Summit Declaration" (Lisbon, Portugal: North Atlantic Council, November 20, 2010), https://www.nato.int/cps/en/natolive/official_texts_68828.htm.

[124] "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization."

[125] "Defending the Networks: The NATO Policy on Cyber Defence" (NATO, 2011), https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

[126] "Defending the Networks: The NATO Policy on Cyber Defence."

in the 2010 Cyber Coalition exercise.[127] The 2010 exercise was NATO's third cyber defense exercise, and only the second iteration open to participation from all Allied nations. The focus of the exercise was to streamline incident response and inter-agency collaboration. Thirteen NATO member states participated in Cyber Coalition 2010 with their own cyber defense capabilities to exercise collaborating with Allies and NATO institutions.[128] The exercise also allowed Alliance members to "practice the consultation and decision-making mechanisms for the RRTs."[129] The RRT concept was subsequently developed throughout 2011, with the intention of fully operationalizing RRTs by the end of 2012.

Over the next few years, NATO continued to integrate cyber defense planning into its broader institutional mechanisms. In April 2012, the Alliance consolidated cyber defense in the NATO Defense Planning Process (NDPP), whereby key "cyber defense requirements are identified and prioritized through the defense planning process."[130] The NDPP is an extensive system by which Allies voluntarily "harmonise their national defence plans with those of NATO."[131] Later that year at the Chicago Summit, NATO reaffirmed its Lisbon Declaration commitments and emphasized that the NCIRC would become fully operational by the end of 2012. RRTs were not specifically mentioned, but cyber defense made a few cameo appearances in the deterrence and defense posture review.[132] In July 2012, the NATO Communications and Information Agency (NCI) was established.[133] The new agency, headquartered in Brussels and The Hague, was the result of a merger of several NATO communications and information agencies.[134] The NCIRC was also folded into NATO's command structure, and would come to house the RRTs.

In February 2014, Allied defense ministers tasked NATO with developing a new cyber policy focused on improving collective defense, increasing assistance to allies, streamlining governance structures, and revamping relations with industry.[135] In May, NATO announced that the NCIRC had reached full operational capacity.[136] A month later at a meeting in Brussels, NATO defense ministers endorsed the new cyber defense policy, the third such document from the Alliance in only six years.[137]

At the Wales Summit in September, NATO elevated cyberattacks as a potential rationale for invoking Article 5, making explicit its earlier statements from 2011. The Wales Summit Declaration noted:

> "Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. **Their impact could be as harmful to modern societies as a conventional attack.** We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."[138]

This was the first time that NATO had specifically mentioned Article 5 in the context of cyberspace operations and attacks.[139] The Alliance also drew a clear equivalency between cyber and kinetic attacks, another first.

In 2015, NATO further institutionalized collective mechanisms for cyber defense, launching Memorandums of Understanding on Cyber Defence to be signed between the Alliance and the national cyber defense authorities of each of the 28 member states at the time.[140] By May 2017, 21 Allies had signed on.[141] Although RRTs were not explicitly mentioned in the press coverage of this move, MOUs are an important legal mechanism for collaboration and have been identified previously as an important element of any further RRT development.

In February 2016, NATO and the EU concluded a Technical Arrangement on Cyber Defence, which established new

---

[127] "NATO Rapid Reaction Team to Fight Cyber Attack"; "'Cyber Coalition 2010' to Exercise Collaboration in Cyber Defence," *NATO Press Release*, 16 November 20110, https://www.nato.int/cps/en/natohq/news_68205.htm?selected-Locale=en.

[128] "Cyber Coalition 2010 Tests NATO's Joint Efforts during Simultaneous Cyber Attacks," *NATO Press Release*, November 16, 2010, https://www.nato.int/cps/en/natolive/news_69805.htm.

[129] "NATO Rapid Reaction Team to Fight Cyber Attack."

[130] "NATO Summit Guide," 127.

[131] "NATO Summit Guide," 150.

[132] "Chicago Summit Declaration" (Chicago, Illinois, United States: North Atlantic Council, May 20, 2012), https://www.nato.int/cps/en/natohq/official_texts_87593.htm?mode=pressrelease; "Deterrence and Defence Posture Review" (Chicago, Illinois, United States: NATO, May 20, 2012), https://www.nato.int/cps/en/natohq/official_texts_87597.htm?mode=pressrelease.

[133] "NATO Summit Guide," 127.

[134] "About Us," NATO Communications and Information Agency, accessed April 2, 2023, https://www.ncia.nato.int/about-us.html.

[135] "NATO Summit Guide," 127.

[136] "NATO Summit Guide," 127.

[137] "NATO Summit Guide," 128; "NATO Summit Updates Cyber Defence Policy," *NATO CCDCOE*, 2014, https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/.

[138] "Wales Summit Declaration" (Wales, United Kingdom: North Atlantic Council, September 5, 2014), https://www.nato.int/cps/en/natohq/official_texts_87597.htm?mode=pressrelease. Emphasis added.

[139] Steve Ranger, "NATO Updates Cyber Defence Policy as Digital Attacks Become a Standard Part of Conflict," *ZDNet*, June 30, 2014, https://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/.

[140] "NATO Summit Guide," 126.

[141] Shea, "NATO: Stepping up Its Game in Cyber Defence."

information sharing mechanisms and collaboration vehicles between NATO's NCIRC and CERT-EU at the non-classified level.[142] At that point in time, the EU was in the process of developing its own rapid response capability for cyber defense, and the two organizations were strengthening ties on cyber defense for several years already. At the Warsaw Summit in June, cyber was declared an operational warfighting domain, becoming the fourth in addition to air, land, and sea.[143] As Jamie Shea, former NATO Deputy Assistant Secretary General for Emerging Security Challenges, noted, this move "shifts the focus from information assurance to mission assurance – or, in other words, from a focus on protecting its own internal networks to a focus on the cyber defence of every military activity that it carries out."[144] At the Summit, NATO also launched a Cyber Defense Pledge designed to inspire Allies to improve their own cyber defense capabilities in line with the two percent of annual GDP on defense commitment benchmarked at the 2014 Wales Summit. The Cyber Defence Pledge thus "commits Allies to spend at least a portion of this extra investment on improving national cyber defences, even if there is no specified minimum amount."[145]

In February 2017, NATO defense ministers approved a plan for the steps needed to bring the new domain concept to fruition by 2019. This roadmap provided for a more tight-knit relationship between Allied Command Operations (ACO) and the NATO Communication and Information Agency (NCIA) in The Hague, which oversees the daily protection and monitoring of internal NATO Networks. The roadmap was built to "ensure a smooth transition from civilian to military responsibility in a crisis situation."[146] NATO also began investing in a back-up NCIRC.[147]

In 2018, NATO established a Cyberspace Operations Centre (CyOC) within Allied Command Operations at the Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium.[148] CyOC was stood up because the Allies "agreed that NATO can draw on national cyber capabilities for its operations and missions. Allies maintain full ownership of those contributions, just as Allies own the tanks, ships and aircraft in NATO operations and missions."[149] CyOC also became responsible for providing ACO and other NATO institutions (such as the NCIRC) with comprehensive situational awareness on the alliance's threat landscape in cyberspace.[150]

The structure of CyOC has its own challenges. For most cyber operations, NATO does not have commonly owned assets but instead relies on national capabilities contributed to the Alliance. NATO members also "retain command and control of cyber operations they provide."[151] This logistical balancing act can cause serious issues in coordinating cyber operations.

There are practical reasons for leaving cyber tools in the hands of those who have created them. First, of course, cyber weapons are not multi-use in the same way as airplanes or battleships. Once used, a cyber effects operation is in the wild and in most instances can be studied and replicated by the target and others. Additionally, a particular exploit or payload may be extremely tailored to a specific target; the design and development process can be incredibly involved, leaving those who were directly responsible for creating the operation in the best position to understand and execute it. Such knowledge is not as easily transferred to a different command and control structure; unlike a bomber or a tank, you cannot necessarily easily teach its maneuverings to a wider audience.

For some former NATO officials and observers, this poses a significant problem in developing a robust cyber program. By leaving cyber weapons in the hands of their creators, rather than moving them under a unified NATO structure, many have argued that the NATO commander does not have the necessary in-depth visibility into the operations they are leading.[152] Although the Supreme Allied Commander Europe (SACEUR) and other top NATO leaders at CyOC will likely have visibility into the broader operational structure, they will not be able to see the tactical and technical procedures that underpin the cyber mission. This may make NATO offensive cyber operations difficult to conduct in the future.

---

[142] "NATO Summit Guide," 128; Jamie Shea, "How Is NATO Meeting the Challenge of Cyberspace?," *Prism* 7, no. 2 (2017): 19–29.

[143] "Warsaw Summit Communiqué" (Warsaw, Poland: North Atlantic Council, July 8, 2016), https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[144] Shea, "NATO: Stepping up Its Game in Cyber Defence," 167.

[145] Shea, "How Is NATO Meeting the Challenge of Cyberspace?," 22.

[146] Shea, 21.

[147] Shea, "How Is NATO Meeting the Challenge of Cyberspace?"

[148] "Brussels Summit Declaration," para. 29.

[149] "Cyber Defence."

[150] Alberto Domingo, "NATO Cyberspace Operations" (NATO Supreme Allied Commander Transformation, Brief to Maritime Security Regimes Round Table, Norfolk, VA, 2019), http://www.cjoscoe.org/infosite/wp-content/uploads/2019/05/NATO-Cyberspace-Operations.pdf.

[151] Sophie Arts, "Offense as the New Defense: New Life for NATO's Cyber Policy," *GMF: Strengthening Translatlantic Cooperation* (blog), December 13, 2018.

[152] Thomas E. Ricks and Rizwan Ali, "NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons," *Foreign Policy*, December 7, 2017, https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/.

At the 2021 Brussels Summit, NATO reaffirmed that a cyberattack could trigger an invocation of Article 5. The Communique asserted:

> "We reaffirm that a decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis. Allies recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack."[153]

Finally, the Communique endorsed the new Comprehensive Cyber Defense Policy, which marked the fourth major cyber defense policy overhaul by NATO.[154] This new policy included an explicit mention of a 24-hour response capability, noting that Rapid Reaction Teams would be on standby.

In 2022 at the Madrid Summit, NATO released its new strategic concept, which strengthened the support package offered to Ukraine, including improving the country's cyber defenses and resilience. The Madrid Summit also established a new virtual rapid response capability:

> "Allies have decided, on a voluntary basis and using national assets, to build and exercise a virtual rapid response cyber capability to respond to significant malicious cyber activities."[155]

Lithuania has offered to take on a leadership role in the NATO RRT force, noting that it has successfully led the EU PESCO project for several years. In a press conference in June 2023, the Vice Minister of National Defense Greta Monika Tuckute stated, "as a member state with significant experience in leading the EU Cyber Rapid Response Teams, Lithuania undoubtedly has know-how and experience to contribute."[156]

4.2 Structure

The North Atlantic Council (NAC) provides high-level political oversight of all major operations and policies implemented by the Alliance, including cyber defense. The NAC is thus "apprised of major cyber incidents and attacks, and it exercises principal authority in cyber defence-related crisis management."[157]

The Cyber Defence Committee is subordinate to the NAC and is the lead committee for cyber defense policy governance. The Committee provides "oversight and advice to Allied countries on NATO's cyber defence efforts at the expert level."[158] Originally, this committee was called the Defence Policy and Planning Committee / Cyber Defence; however, in 2014, the NAC restructured the planning process, creating the separate Cyber Defence Committee. The Cyber Defence Committee plays a key role in linking broad political strategy as defined by the NAC with the technical operating level of NATO institutions. The Committee provides "the essential link between the technical operating level and the policymaking level, without which progress would be ad hoc and uncoordinated."[159]

Below the Cyber Defence Committee sits the NATO Chief Information Officer (CIO). Previously, NATO had instituted a Cyber Defence Management Board (CDMB) to coordinate cyber defense at the working level across all NATO civilian and military bodies. However, the CDMB was dissolved in 2021 after an extensive cyber adaptation program was implemented to improve network defense across all NATO enterprises.[160] The Brussels Summit established the new CIO position, with Manfred Boudreaux-Dehmer appointed as the first CIO in September 2021.[161]

The cyber adaptation program created the Office of the CIO to serve as a single point of authority for all cyber risk management across NATO. The CIO:

> "facilitates the integration, alignment and cohesion of Information and Communications Technology (ICT) systems NATO-wide, and

[153] "Brussels Summit Communiqué" (Brussels, Belgium: North Atlantic Treaty Organization, June 14, 2021), para. 22, https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.

[154] "Brussels Summit Communiqué," para. 32.

[155] "Madrid Summit Declaration" (Madrid, Spain: North Atlantic Council, June 29, 2022), para. 10, https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

[156] "We Have Emerged Stronger from Challenging Situations but We Remain Vigilant, Vice Minister G. M. Tuckute Describes the State of Cybersecurity in Lithuania," *Ministry of National Defence Republic of Lithuania*, June 1, 2023, Online edition, https://kam.lt/en/we-have-emerged-stronger-from-challenging-situations-but-we-remain-vigilant-vice-minister-g-m-tuckute-describes-the-state-of-cybersecurity-in-lithuania/.

[157] "NATO Summit Guide," 126.

[158] "NATO Summit Guide," 126.

[159] Shea, "How Is NATO Meeting the Challenge of Cyberspace?," 25.

[160] Senior NATO Official, Author Interview on NATO Cyber Rapid Response Teams.

[161] "Manfred Boudreaux-Dehmer," NATO, November 15, 2021, https://www.nato.int/cps/en/natohq/who_is_who_188597.htm?; "Brussels Summit Communiqué," para. 77.

> oversees the development and operation of ICT capabilities. The CIO is also the single point of authority for all cyber security issues throughout NATO. This includes leading incident management, orienting specific investments, improving NATO's cyber security posture, as well as increasing cyber security awareness NATO-wide."[162]

The CIO manages the NCIRC, which provides the experts who eventually compose an RRT team. An RRT team consists of a permanent core of six specialists, including national or NATO experts in specific skill areas. As with the EU CRRTs, their exact profiles are dependent on the incident that the RRT is deployed to assist. The RRT team is built out of NCIRC employees. The NCIRC is staffed by 200 specialists. However, the RRT team is not a static composition. RRTs are constructed from permanent NCIRC staff at the time of activation. As one NATO official noted, "it's not a bunch of dudes or dudettes sitting in a basement waiting to be deployed… they are hands on keyboards and part of the 200 strong NCIRC team that does NATO enterprise network protection."[163]

Requests for assistance must be approved by the North Atlantic Council, meaning that all 31 NATO Allies are privy to RRT deployment decisions. RRTs are also intended to be deployable within 24-hours of an incident.[164]

4.3 Purpose & Use Cases

The primary purpose of the RRTs is to protect NATO's own internal networks.[165] These networks cover a vast geographic area – the NCIRC is responsible for tackling cyber incidents in NATO infrastructure stretching from Allied Land Command in Izmir, Turkey, to the Joint Force Command in Norfolk, Virginia – making a deployable force a useful option. RRTs are also meant to be a capability that can be marshalled to support struggling Allies. As Jamie Shea, former Deputy Assistant Secretary General for Emerging Security Challenges at NATO Headquarters, has articulated:

> "The starting point for this effort is the recognition that every future crisis or conflict will have a cyber dimension, and that just as NATO has had to build missile defense and conventional postures into its traditional nuclear-based deterrence strategy, it will need to increasingly incorporate cyber expertise and capabilities as well."[166]

The Alliance has had some internal confusion over possible use cases for RRT activation, however. In a 2012 blog released on NATO's main website, RRTs were described as a tool to be used to aid stricken Allies, noting that, "any NATO member nation suffering a significant cyber attack will be able to ask for NATO's help."[167] Yet, in 2013, then-NATO Secretary General Anders Fogh Rasmussen wrote in a piece in *The Wall Street Journal* that the teams were first and foremost for defending NATO networks. He noted, "a possible next step could be to make such teams available on request to NATO countries."[168] NATO has still not fully clarified this issue a decade later. Although in recent years, NATO has begun speaking of the RRT and now the virtual RRT capability as deployable to requesting Allies, the teams have never been sent abroad to deliver aid to an Ally.[169]

The Alliance has a handbook outlining possible use cases for the RRTs, but it is an internal document rather than an agreed political framework. As such, it has never been made public. Primarily, the handbook covers deployment issues and roles and responsibilities, and serves as a working document for the NCIRC.[170]

4.4 Implementation Challenges

RRTs are also meant to be deployed reactively and defensively to remediate crisis situations. NATO already has a shared resource in the NCIRC designated for possible deployment. These RRTs are drawn from the NCIRC within the NCIA and are thus a commonly funded NATO asset. This contrasts with the EU CRRT program, which is funded by the member states participating in the specific PESCO project (primarily the lead state and the hosting state). Arguably, the CRRT set-up could be more well-suited to promote project buy-in.

RRTs instead face additional political hurdles because they are composed of a financially pooled NATO resource. Any deployment of RRT activation will be a question of

[162] "Cyber Defence."

[163] Senior NATO Official, Author Interview on NATO Cyber Rapid Response Teams.

[164] "NATO Rapid Reaction Team to Fight Cyber Attack."

[165] Anders Fogh Rasmussen, "NATO's Next War - in Cyberspace," *The Wall Street Journal*, June 3, 2013, Europe Edition edition.

[166] Shea, "How Is NATO Meeting the Challenge of Cyberspace?," 20.

[167] "NATO Rapid Reaction Team to Fight Cyber Attack."

[168] Rasmussen, "NATO's Next War - in Cyberspace."

[169] Senior NATO Official, Author Interview on NATO Cyber Rapid Response Teams, 22 March 2023.

[170] Senior NATO Official.

resource allocation: can the NCIRC spare specialists for an RRT mission, or will activation of a team reduce the organization's effectiveness? Will an RRT be mobilized efficiently? Will RRT deployment be fairly allocated across NATO members and partners?

RRTs also experience challenges stemming from the tight control of information related to cyber threats and operations. While RRTs do not need to gather tactical details for offensive operations, they do need to access sensitive cyber threat intelligence. Individual Allies tend to control cyber intelligence more tightly than other forms of intelligence, often because such information was gathered through sensitive and covert means. In many cases, such information is not even shared internally across a nation's government institutions, much less with external stakeholders.[171]

NATO RRTs also must be able to have detailed information about the systems and infrastructure they need to remediate. For an RRT to work, a state or institution undergoing a crisis must be willing to share highly sensitive information about both the nature of the threat they face *and* the technical workings of their systems, opening up networks and ICT infrastructure to extensive scrutiny. NATO institutions are in a much better position to share this information with the NCIRC, since they are already interfacing with the facility on a somewhat regular basis. Gaining access to allied and NATO partner country networks, however, is likely more challenging. If states are not willing to hand over this kind of tightly controlled information, then RRTs will be handicapped from the start.

Countries across NATO have very different levels of cybersecurity defenses, even across government and military institutions. Some states may need RRTs more frequently than others because they do not have robust cyber defenses already implemented at home. Allies with stronger cyber defense capabilities may also be reluctant to share sensitive intelligence with a stricken member state, who they cannot guarantee will safeguard such intelligence closely enough to prevent it from falling into adversarial hands. Trust relationships among NATO allies are also far from perfect, and political grievances and skepticism abound. A Turkish RRT member might be regarded with suspicion if they join onto a team deploying to Greece; likewise, following the fallout from the Snowden leaks, a US member might not be greeted with open arms in a deployment to Germany.

The Cyber Defence Pledge has been instituted to help remedy this problem – at least, the financial aspect. However, the Pledge is still in its infancy. The Pledge was first launched in 2016, building from the commitment made by Allies two years earlier to spend at least two percent of their GDP on defense. The cyber element of this increased spending was not fully articulated. Allies needed to commit to "at least a portion of this extra investment on improving national cyber defences, even if there is no specified minimum amount."[172]

Allies have begun developing self-assessments of cyber defense hygiene, reporting on several capability areas:[173]

Strategy
Organization
Processes and procedures
Threat intelligence
Partnerships
Capabilities
Investments

However, these seven areas are still quite broad. Prioritization is not immediately evident – should countries focus first on developing a sufficient strategy before moving on to capabilities and investments? Although the creation of benchmarks from advanced to "relative beginner" are helpful, there is still much to be developed here.[174]

As mentioned previously, deployment of an RRT is a political decision made at the level of the NAC. All NATO allies must reach a consensus to deploy a team. As one NATO official has said, "this is a key decision – you're not only talking about technical assistance but about signaling."[175] Sending an RRT is a political decision that sends a political message about resourcing and priorities to both adversaries and allies alike.

Finally, any RRT deployment involves key questions of liability. If an RRT is unable to remediate a threat, who is responsible? What if an RRT does more harm than good – what kind of legal and political liabilities arise? Since the RRT capability has never been activated outside of exercises, these questions remain unanswered.

[171] Ricks and Ali, "NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons."

[172] Shea, "How Is NATO Meeting the Challenge of Cyberspace?" 22.

[173] Shea, 23.

[174] Shea, 23.

[175] Senior NATO Official, Author Interview on NATO Cyber Rapid Response Teams.

5 Case Studies

Thus far, neither NATO nor EU rapid response teams have been deployed in a crisis. NATO RRTs have only ever been activated during exercises, and EU CRRTs have only been sent abroad to partner countries to conduct vulnerability assessments and help bolster cyber defense and cybersecurity capabilities in long-term resilience efforts.

This section looks at four case studies: Ukraine, Albania, Moldova, and Mozambique. In the Ukrainian case, an EU CRRT was ready to deploy but was ultimately delayed due to the Russian invasion in late February 2022. In the case of Albania, NATO appears to have discussed some kind of response, but no RRT was ever sent. And finally, in both the Moldova and Mozambique cases, CRRTs were sent as part of the EU's broader partner missions.

5.1 Ukraine 2022

As early as January 2022, the EU's High Representative (HR), Josep Borrell, signaled that the institution would investigate employing a PESCO CRRT project to aid Ukraine. Ukraine had been hit by a major cyberattack against government websites, shutting down the ministry of foreign affairs and education ministry sites altogether. In remarks given at Brest, France on 14 January, Borrell said:

> "We, the Member States, have the rapid response cyber unit, that is to say, the capacity to act in rapid response to this kind of attack, and we will mobilize them. And we have a PESCO project which precisely deals with the way in which we can defend against cyber attack. I am going to ask the Member States that, even if Ukraine is not a member of the European Union and does not take part in this project, we could mobilize the resources that we have in order to deal with this sort of offensive. So we will mobilize all resources to help Ukraine deal with this cyber attack. Unfortunately, we expected that to happen."[176]

The HR then issued a declaration on behalf of the EU condemning the cyberattacks against Ukraine and reiterated pledging support, stating that, "the European Union and its Member States are in contact with Ukraine and stand ready to provide additional, direct, technical assistance to Ukraine to remediate this attack and further support Ukraine against any destabilizing actions, including by further building up its resilience against hybrid and cyber threats."[177]

The full activation of a CRRT team took well over a month. Although the HR made clear his desire for such a deployment, the official process had to be run through the CRRT project and its member states. First, a formal Ukrainian request needed to be submitted to the CRRT Council. Next, the CRRT Council had to convene and vote on the request for assistance. Usually, the Rotating Partner (RP) co-chairs the Council along with Lithuania; as the RP changes in January of each year, Romania had likely just taken over its duty as RP for 2022 when Ukraine requested assistance.

Both the request from Ukraine and the convening of the Council appeared to have taken some time. In February 2022, Denmark extended a unilateral offer of support to Ukraine, raising the possibility of sending five to ten cyber advisors to Ukraine to help protect critical infrastructure.[178] Kyiv, meanwhile, seemed unaware of these purported offers of assistance. Viktor Zhora, Deputy Chairman and Chief Digital Transformation Officer at the State Service of Special Communication and Information Protection of Ukraine (SSSCIP), told reporters that he had not received any information about a Danish overture.[179]

Finally, on Friday, 18 February, the Ukrainian government asked for cyber military support from the EU in a formal letter.[180] Ukraine's Foreign Minister Dmytro Kuleba wrote to EU leaders that the country "would 'welcome

[176] Google Translate, trans., "Informal meeting of foreign ministers (Gymnick): Remarks by High Representative / Vice-President Josep Borrell upon arrival," Press Release, European Union External Action, January 14, 2022, https://www.eeas.europa.eu/eeas/r%C3%A9union-informelle-des-ministres-des-affaires-%C3%A9trang%C3%A8res-gymnich-remarques-du-haut_en?page_lang=en. Translated using google translation services. Original remarks : «Nous avons, les États membres, the rapid response cyber unit, c'est à dire, de capacité d'agir en réponse rapide à cette sorte d'attaque, et on va les mobiliser aussi. Et nous avons un projet PESCO qui justement traite de la façon dont on peut faire la défense contre l'attaque cybernétique. Je vais demander aux États membres que, même si l'Ukraine n'est pas membre de l'Union européenne et ne participe pas dans ce projet, on pourrait mobiliser dans son aide les ressources que nous avons pour faire face à cette sorte d'attaque. Donc on va mobiliser toutes les ressources pour aider à l'Ukraine à faire face à cette attaque cybernétique. Malheureusement, on s'attendait à que ça puisse arriver.»

[177] Council of the EU, "Ukraine: Declaration by the High Representative on Behalf of the European Union on the Cyberattack against Ukraine," Press Release, European Union Council of the European Union, January 14, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/.

[178] Mads Korsager Nielsen and Henrik Moltke, "After massive hacker attacks: Confusion about Danish cyber aid to Ukraine," *DR*, February 20, 2022, 8 April 2023, https://www.dr.dk/nyheder/indland/efter-massive-hackerangreb-forvirring-om-dansk-cyber-hjaelp-til-ukraine.

[179] Nielsen and Moltke.

[180] Lauren Cerulus, "EU to Mobilize Cyber Team to Help Ukraine Fight Russian Cyberattacks," *Politico*, February 21, 2022, Politico Pro Online edition, n. quoting Kuleba, https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/.

deployment to Kyiv' of the 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'."[181]On Monday, 21 February, EU HR Josep Borrell announced that the EU would send a CRRT to help Ukraine after meeting with Kuleba.[182]

On 22 February 2022, the CRRT Council confirmed that the capability would be activated to support Ukraine. The participating member states – Lithuania, The Netherlands, Poland, Estonia, Romania, and Croatia – voted to respond affirmatively to a request submitted by Ukraine.[183] This event marked the first time that a CRRT had been activated to assist a state in an ongoing crisis scenario. According to Lithuania's Vice Minister of National Defense, Margiris Abukevičius, the CRRT was activated to "'support Ukraine's institutions in the face of cybersecurity challenges.'"[184]

In a tweet from its Ministry of Defense, Lithuania announced that it would head the team as the lead participant on the project.[185] A team of eight to twelve experts were convened to provide support to Ukraine both virtually and on-site. Later reporting suggests that the final team consisted of ten experts.

Yet, the actual logistics of deployment unfolded slowly. The CRRT was set to travel to Kyiv within a week of the announcement of assistance for an "initial exploration of the Ukrainian networks."[186]

European Defense Agency Twitter, 24 February 2022

However, two days after the announcement – and on the very day the CRRT was set to leave for Kyiv – Russia invaded Ukraine. The team began scrambling to find other possible avenues to provide aid, including through remote digital support efforts.[187]

Ultimately, the CRRT was not deployed to Ukraine. The escalating situation undoubtedly played a significant role in this eventuality: the Council appeared to decide against sending its team into an active warzone. However, the lengthy delay (from mid-January to late February) between initial consideration and activation of the team certainly played a part as well. While the Council had previously agreed to respond to requests for help within 24 hours, in this case the political decision to act took much longer. While the request for assistance officially came in on 18 February, the idea had been raised both formally by the EU HR in mid-January, and informally by Ukrainian government officials. The turnaround time between formal request and activation seems to have only taken about four days; however, this ignores the extensive and timely back-channel communications that led to the initiation of the formal request. Regardless, it seems clear that the EU CRRT process has not lived up to its goal of 24-hour response times.

On a positive note, the CRRT Council was able to select specialists to send to Kyiv. The Dutch member had already been chosen and was set to travel before the Council pulled the plug on the enterprise.

NATO also mobilized to aid Ukraine in the wake of the Russian invasion. Secretary General Jens Stoltenberg announced, "in response to Russia's massive military buildup over the past months, we have all of us strengthened our deterrence and defense… We are deploying elements of the NATO Response Force on land, at sea and in the air, to further strengthen our posture and to respond quickly to any contingency."[188] However, Stoltenberg made no mention of supporting Ukrainian cyber defenses, instead focusing on conventional military support (land, sea, and air).

In the case of Ukraine, support for digital infrastructure has tended to come not from multilateral institutions like the EU and NATO, but from individual nations and private companies. The UK mobilized massive resources to support Ukraine, including through a £6 million support package.[189] Meanwhile, in the private sector, major tech

[181] Cerulus, "EU to Mobilize Cyber Team to Help Ukraine Fight Russian Cyberattacks."

[182] Cerulus.

[183] "EU Cyber Rapid Response Teams to Support Ukraine."

[184] "EU Cyber Rapid Response Teams to Support Ukraine"; Tomislav Krasnec, "Croatia Sends Cyber Warriors to Help Ukraine: This Is Hte First Time This Defense Project Has Been Activated," *Vecernji List*, February 22, 2022, https://www.vecernji.hr/vijesti/hrvatska-salje-cyber-ratnike-u-pomoc-ukrajini-ovo-je-prvi-put-da-je-aktiviran-taj-obrambeni-projekt-1565517.

[185] Joe Tidy, "Ukraine: EU Deploys Cyber Rapid-Response Team," *BBC*, February 22, 2022, online edition, https://www.bbc.com/news/technology-60484979.

[186] "Ukraine Accepts Dutch Offer of Help against Cyber Attacks," *NL Times*, February 22, 2022, https://nltimes.nl/2022/02/22/ukraine-accepts-dutch-offer-help-cyber-attacks.

[187] "Ukraine Accepts Dutch Offer of Help against Cyber Attacks."

[188] Henry Ridgwell, "NATO Triggers Rapid Response Force as Russian Forces Advance on Kyiv," *VOA News*, February 25, 2022, https://www.voanews.com/a/nato-triggers-rapid-response-force-as-russian-forces-advance-on-kyiv-/6459908.html.

[189] "UK Boosts Ukraine's Cyber Defenses with £6 Million Support Package," *UK Foreign, Commonwealth & Development Office* (blog), November 1, 2022,

companies have made even bigger financial commitments to the country. Microsoft has announced that it has spent over $400 million in defending Ukrainian ICT systems since the onset of the war in February.[190]

Indeed, individual countries and tech corporations have been able to move much more quickly than NATO or the EU to aid Ukraine. The Ukrainian case emphasizes some of the potential shortcomings of the CRRT and RRT processes, which take time to implement and involve political buy-in from several countries – or, in the case of NATO, from all 31 Allies.

In November 2022, the EU launched a new Cyber Defence policy and Action Plan on Military Mobility 2.0, which was explicitly engineered to "address the deteriorating security environment following Russia's aggression against Ukraine and to boost the EU's capacity to protect its citizens and infrastructure."[191] One of the major tenets of the new policy was to invest in cyber defense capabilities, including "cooperative platforms and funding mechanisms" like PESCO. In the Joint Communication, the CRRT project was called out by name, as the EU Commission and member states set out to explore possibilities for its expansion to better support EU member states and CSDP missions.[192] The document does not explicitly mention the CRRT's failed efforts in Ukraine, but it does make clear that the ongoing conflict in Ukraine is a significant threat to both member states' cybersecurity and to broader CSDP missions central to the EU.

5.2 Albania 2022

Over the summer of 2022, Albania experienced several significant cyberattacks against its government institutions. The first attack occurred in May, targeting the government service administrate.al. In July, further attacks occurred against the government portal e-albania.al, the site where citizens can log in using state identification and apply for official documents.[193]

The attacks were eventually attributed to Iran.[194] On 6 September, the Albanian government officially severed diplomatic ties with the Islamic Republic of Iran, giving all diplomatic staff at the Embassy in Tirana 24 hours to vacate the country.[195] This incident marked the first time a country had cut diplomatic ties over a cyberattack.[196]

Albania looked to NATO for support after the attacks, including raising the possibility of invoking Article 5 of the Washington Treaty. Edi Rama, Prime Minister of Albania, compared the cyberattacks to a conventional strike, noting that "It's like bombing a country."[197] A significant proportion – up to 95% -- of government services in the country are provided online, meaning that the attacks severely handicapped daily life in the country.

Ultimately, however, Albania decided against pushing for Article 5 deliberations. In an interview with Politico, Rama said, "'I have too much respect for our friends and our allies to tell them what they should do… We are always very careful to be very humble in our assessments.'"[198]

Once again, neither a NATO RRT nor an EU CRRT was invoked to aid Albania. The High Representative issued a declaration on behalf of the EU, expressing solidarity with the country and "strongly condemn[ing] such unacceptable behaviour in cyberspace, which goes against agreed norms of responsible state behaviour, as repeatedly endorsed by all UN Member States."[199]

https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package.

[190] Brad Smith, "Extending Our Vital Technology Support for Ukraine," *Microsoft* (blog), November 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/.

[191] European Commission, "Cyber Defence: EU Boosts Action against Cyber Threats," Press Release, European Commission, November 10, 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6642.

[192] High Representative of the Union for Foreign Affaris and Security Policy, "Joint Communication to the European Parliament and the Council," EU Policy on Cyber Defence (Brussels, Belgium: European Commission and HR, November 10, 2022), 6, https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf.

[193] Elona Elezi and Niloofar Gholami, "Albania Blames Iran for Cyberattacks," *DW*, September 16, 2022, https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285.

[194] "Homeland Justice Operations against Albania (2022)," *Cyberlaw Toolkit, CCD-COE* (blog), February 2, 2023, https://cyberlaw.ccdcoe.org/wiki/Homeland_Justice_operations_against_Albania_(2022); "Iranian State Actors Conduct Cyber Operations Against the Government of Albania," Cybersecurity Advisory (CISA, September 23, 2022), https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a; Sean Lyngaas, "Albania Blames Iran for Second Cybreattack since July," *CNN*, n.d., 12 September 2022 edition, https://edition.cnn.com/2022/09/10/politics/albania-cyberattack-iran/index.html.

[195] Elezi and Gholami, "Albania Blames Iran for Cyberattacks."

[196] Tim Starks, "Albania Is the First Known Country to Sever Diplomatic Ties over a Cyberattack," *The Washington Post*, September 8, 2022, The Cybersecurity 202 edition, https://www.washingtonpost.com/politics/2022/09/08/albania-is-first-known-country-sever-diplomatic-ties-over-cyberattack/.

[197] Maggie Miller, "Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack," *Politico*, October 5, 2022, https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347.

[198] Miller.

[199] "Cyber-Attacks: Declaration by the High Representative on Behalf of the European Union Expressing Solidarity with Albania and Concern Following the July Malicious Cyber Activities," Press Release, European Council and Council of the European Union, September 8, 2022,

The statement made no mention of the use of CRRTs or any specific support mechanism. Instead, the High Representative noted that, "in line with the EU Cybersecurity Strategy and Strategic Compass, the European Union is determined to prevent cyberattacks through enhanced resilience and by responding firmly to cyberattacks against the EU and its member states and is committed to assisting building up cyber security resilience in candidate and other countries, using all available EU tools. We continue to monitor the situation carefully and stand ready to take further steps where necessary to support Albania."[200]

Albania continues to be a candidate country for EU membership, not a full-fledged member state. This may have impacted the declaration and shaped any decisions or discussions surrounding the use of a CRRT. To date, no evidence exists of serious deliberation around the possible deployment of a CRRT in fall 2022 to Tirana.

NATO was fairly muted in its defense of Albania as well. On 8 September, the North Atlantic Council released its own statement of solidarity, also "strongly condemn[ing] such malicious cyber activities designed to destabilise and harm the security of an Ally, and disrupt the daily lives of citizens."[201] The statement included references to strengthening cyber defense capabilities, but it did not make any mention of the NATO Cyber Rapid Reaction Teams or related capabilities.

On 21 September, NATO officials met with Albanian Defence Minister Niko Peleshi in Tirana to "assess the recent cyber attack on Albania's national information infrastructure and discuss further NATO support."[202] Once again, the NATO press release included broad allusions to support but no concrete steps. Indeed, it seems more likely that this additional statement and NATO visit arose at least in part from the Albanian president's discussion of invoking Article 5. By October, President Rama had ceased such public deliberations, instead deferring to the alliance. It is possible that he found little support for the idea among the North Atlantic Council.

While neither NATO nor the EU PESCO project deployed a rapid response team, an incident response capability was sent to Albania. The United States launched a hunt forward team to the country to provide support through its Cyber National Mission Force (CNMF). US specialists were sent to Albania for three months to provide assistance in the wake of the attacks. This marked the first time that the US had sent a defensive hunt forward team to Albania. US Cyber Command (CYBERCOM) announced that the operation had taken place in March of 2023.[203] Nathaniel Fick, the US Ambassador at Large for Cyberspace and Digital Policy, stated:

> "The United States is committed to working with Albania on securing its digital future, and ensuring that connectivity is a force for innovation, productivity, and empowerment… We will continue to support our NATO ally Albania's remediation efforts, and invite partners to join us alongside our NATO allies in holding Iran accountable for its destructive cyberattacks against Albania in July and September 2022."[204]

Once again, the Albanian case study underscores the flexibility of unilateral action to aid an afflicted state. While the NATO RRT involves a political decision at the level of the NAC, the US was able to invoke its CNMF operators much more quickly and decisively.

As of March 2023, the US has deployed the CNMF 44 times to 22 countries, conducting hunt forward operations on close to 70 different networks. Teams have been deployed to Croatia, Estonia, Lithuania, Montenegro, North Macedonia, Ukraine, and other countries since the project was operationalized in 2018.[205] This stands in stark contrast to the NATO RRT capability, which has yet to be deployed to assist a stricken state.

---

https://www.consilium.europa.eu/en/press/press-releases/2022/09/08/cyber-attacks-declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-albania-and-concern-following-the-july-malicious-cyber-activities/.

[200] "Cyber-Attacks: Declaration by the High Representative on Behalf of the European Union Expressing Solidarity with Albania and Concern Following the July Malicious Cyber Activities."

[201] "Statement by the North Atlantic Council Concerning the Malicious Cyber Activities against Albania," Press Release, NATO, September 8, 2022, https://www.nato.int/cps/en/natohq/official_texts_207156.htm.

[202] "NATO Reaffirms Support for Albania Following Cyber Attacks," Press Release, NATO, September 21, 2022, https://www.nato.int/cps/en/natohq/news_207552.htm?selectedLocale=en.

[203] Colin Demarest, "US Sent 'hunt-Forward' Team to Albania in Wake of Iranian Cyberattacks," *C4ISRNet*, March 23, 2023, https://www.c4isrnet.com/cyber/2023/03/23/us-sent-hunt-forward-team-to-albania-in-wake-of-iranian-cyberattacks/#:~:text=Cyber-,US%20sent%20%27hunt%2Dforward%27%20team%20to%20Albania,in%20wake%20of%20Iranian%20cyberattacks&text=WASHINGTON%20%E2%80%94%20U.S.%20cyber%20specialists%20spent,Iranian%20cyberattacks%20on%20government%20systems.

[204] Cyber National Mission Force Public Affairs, "'Committed Partners in Cyberspace': Following Cyberattack, US Conducts First Defensive Hunt Operation in Albania," *U.S. Cyber Command*, March 23, 2023, https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/.

[205] Cyber National Mission Force Public Affairs.

5.3 Moldova 2022-23

Moldova has faced increased cyberattacks since Russia's invasion of Ukraine in February 2022, including Russian-backed cyber-enabled information operations focused on undermining the country's legitimacy and stability.[206] Bordering Ukraine, Moldova has been outspoken in its condemnation of Moscow. The government in Chișinău has also been advocating for EU membership, making it a target of pro-Russian actors.

Moldova has been engaged in several cyber capacity building programs with external partners. Since 2022, these efforts have proliferated. Czechia and Romania have entered into bilateral cyber-assistance programs; Czechia's project is part of a broader series of bilateral agreements with several countries in the region, while Romania has engaged in a specific support program for Moldova, slated to run until February 2026.[207] In May 2022 the EU launched the Moldovan Cybersecurity Rapid Assistance program to increase resilience across public and critical infrastructure sectors.[208] While the project has many capacity development aims, it is not intended to provide support to Moldova's cyber defense.[209]

As early as Fall 2022, the CRRT Council began discussing sending a support team to Moldova. At a high-level meeting at the end of September, plans to support Moldova were eventually endorsed.[210] Lithuanian Vice Minister of National Defense, Margiris Abukevičius stated that the "Cyber Rapid Response Teams can be deployed with the EU or in support of EU partners. We can see that the need to support partners has been growing and at the moment we are prepared to back up Moldova."[211]

In November 2022, the EU CRRT team provided support to Moldova and conducted a vulnerability assessment.[212] The CRRT was deployed both on the ground and through a virtual capacity. As the Lithuanian Ministry of National Defence stated, "this opens the door for testing the capability not only in support of member states and participants of the project, EU authorities, agencies, and institutions, but also EU partners."[213] The specifics of the CRRT activities have not been made public beyond the above stated vulnerability assessment.

In March 2023, the situation in Moldova appeared to escalate. A classified FSB-drafted plan to destabilize Moldova became public, provoking outcry in the country.[214] The plan, which was drafted in 2021, laid out a ten-year plan geared to disrupt Moldova's growing ties to the West and its application to join the European Union, and eventually bring the small former Soviet country back into Russia's orbit.[215]

After receiving a request from the Moldovan government, the EU Council launched the EU Partnership Mission in the Republic of Moldova (EUPM Moldova) on 22 May 2023.[216] This project is the first CSDP mission that has a specific mandate in the field of hybrid threats. The mission is purely civilian in nature. The full EU support package for Moldova, assembled by the European Commission and the European External Action Service, was announced by European Commission President Ursula von der Leyen in Chișinău on 31 May 2023. The support package has two primary objectives: (1) "address the impact of the Russian war of aggression against Ukraine in Moldova" and (2) "bring Moldova closer to the European Union".[217]

In April 2023, the EU CRRT project announced the deployment of a second team to Moldova.[218] Very little is known about this deployment and its objectives, although it has been publicized in the context of the EUPM Moldova and the ongoing EU support mission in the country.

---

[206] Thales Cyber Threat Intelligence Team, "2022-2023: A Year of Cyber Conflict in Ukraine" (Thales, March 2023); Osborne and Jarnecki, "Battening Down the Hatches: Moldova's Cyber Defence."

[207] "CCB Projects Mapping," database, EU CyberNet, 2023, https://www.eucybernet.eu/ccb-table/; Osborne and Jarnecki, "Battening Down the Hatches: Moldova's Cyber Defence."

[208] "Moldova Cybersecurity Rapid Assistance," Project Database, Cybil Portal, accessed August 17, 2023, https://cybilportal.org/projects/moldova-cybersecurity-rapid-assistance/; "Moldova Cybersecurity Rapid Assistance," EGA, 2022, https://ega.ee/project/moldova-cybersecurity-rapid-assistance/#:~:text=The%20European%20Union%20introduced%20Rapid%20Assistance%20Project%20in,aligning%20their%20operations%20with%20the%20EU%20NIS%20Directive.

[209] Osborne and Jarnecki, "Battening Down the Hatches: Moldova's Cyber Defence."

[210] Cemerka, "Ministry of National Defence Preparing Plans for CRRTs to Assist Moldova."

[211] Cemerka.

[212] "Key Trends and Statistics of the National Cyber Security Status of Lithuania 2022," 5.

[213] "Lithuanian-Coordinated EU Cyber Rapid Response Teams - Incident Response with the EU and in Support of EU Partners and Military Missions."

[214] Tim Lister, "Secret Document Reveals Russia's 10-Year Plan to Destabilize Moldova," *CNN*, March 18, 2023, online edition, https://edition.cnn.com/2023/03/16/europe/russia-moldova-secret-document-intl-cmd/index.html; Benkler, "Deploying CSDP Missions to Counter Hybrid Threats - EUPM Moldova: First of Its Kind."

[215] Lister, "Secret Document Reveals Russia's 10-Year Plan to Destabilize Moldova."

[216] "EU Partnership Mission in the Republic of Moldova (EUPM)."

[217] "EU Support Package for the Republic of Moldova" (European Commission and European External Action Service, 2023), https://www.eeas.europa.eu/sites/default/files/documents/2023/Support_Package_Moldova-2806.pdf.

[218] Osborne and Jarnecki, "Battening Down the Hatches: Moldova's Cyber Defence."

5.4 Mozambique 2023

In March 2023, a CRRT was mobilized to Mozambique in support of the European Union Training Mission in the country (EUTM-Moz). The CRRT conducted a vulnerability assessment in the country.[219] According to the government of Lithuania, this deployment was "the first test of CRRT capabilities in the EU Common Security and Defence Policy missions and operations."[220]

Lithuanian MOD Twitter, 30 March 2023

The Mozambique deployment appears to have laid the foundation for the second round of Moldova support in April, although information about both missions remains scarce.

Here, the CRRT was very directly connected with a broader EU mission (EUTM-Moz) and was also sent in a proactive capacity. Rather than responding to a direct or imminent threat, the CRRT was deployed to conduct security measures and training outside of a crisis scenario. It is not known how long it took the CRRT Council to assemble a team or approve its deployment. It seems likely, however, that the proactive nature of the CRRT mission alleviated the kinds of time pressures the Council has faced in the past.

[219] "Key Trends and Statistics of the National Cyber Security Status of Lithuania 2022," 5.

[220] "Lithuanian-Coordinated EU Cyber Rapid Response Teams - Incident Response with the EU and in Support of EU Partners and Military Missions."

6 Conclusion: Rapid Response Teams for Switzerland?

Multinational rapid response teams remain much more of an idea than a reality. Although in the past year, the EU CRRT has begun deploying teams to Moldova and Mozambique, it has done so proactively rather than reactively. In neither case was the CRRT responding to an acute, ongoing crisis. Instead, the CRRT teams conducted vulnerability assessments and other general cyber defense support assignments.

In many ways, this development toward proactive deployment and long-term cyber defense is a welcome step forward. Many NATO and EU officials have been clamoring for the institutions to pay more attention to resilience and capacity-building, rather than focusing all their attention on crisis management. As one NATO official put it, "I don't think that we can patch ourselves out of this, or that a reactive posture will be feasible… We need to focus more on what happens left of the bang."[221]

Yet, the initial goal of a rapid response team is just that – to be a rapid emergency service that can be quickly and nimbly deployed after a major crisis. In this stated mission, multinational teams have fallen well short of the mark. Instead, single-country rapid response teams have proven much more effective. The US Hunt Forward teams have been able to mobilize in response to acute crises, such as the Albanian incident in 2022.

After Montenegro suffered a major cyberattack against its government IT infrastructure in August 2022, the country turned not to NATO or the EU, but to a single country – France – for support.[222] Montenegro has been a NATO member state since 2017; indeed, in the waning stages of its candidacy, the country faced a spate of cyberattacks. Montenegro did alert the alliance of the attack but did not end up making a formal request of the NAC to deploy a rapid reaction force.[223] Montenegro is also an EU candidate country, but there are no records of a request made to the CRRT.

Instead, Montenegro made a formal request to the French government for assistance in "identifying, analysing, and remediating the consequences of cyberattacks against Montenegro that have affected the state information infrastructure since the end of August this year."[224] France mobilized support to the country through its National Cybersecurity Agency (ANSSI).[225] France has been the architect of other cybersecurity capacity-building projects in Montenegro and the Balkans more broadly, including building a new cybersecurity and cybercrime fighting center in the country.[226] This ongoing partnership likely influenced Podgorica's decision to reach out to Paris rather than Brussels or Washington.

In both cases, single country teams have been able to leverage their existing relationships with stricken countries and mobilize quickly and decisively to assist in a crisis. EU CRRTs and NATO RRTs may have well publicized mission sets, but they come with significant bureaucratic baggage. Even the EU CRRT process, which involves only eight countries instead of NATO's 31, has been unable to reach decisions and deployments in reasonable time frames. Instead, the EU CRRTs seem much better equipped to handle longer-term relationship building missions, such as the ongoing deployment in Moldova.

One significant challenge faced by multinational rapid response teams is that they often have mission sets that do not adequately reflect their structure. The EU CRRT is a clear case of such mismatch. Lithuania's PESCO project has articulated several ambitious goals, including integrating the crisis management programs of the eight participating countries into cohesive multinational teams. Indeed, its published frameworks have an explicit preference for teams composed of experts from several participating countries, rather than teams made up of a single PESCO member. Yet, while this goal may be admirable in building EU solidarity and closer ties among participants, it is not always compatible with crisis response. A multinational team needs to have deep insight into the other members' strengths and weaknesses – something that the PESCO project has reportedly had trouble with in the past. The CRRT are

[221] Senior NATO Official, Author Interview on NATO Cyber Rapid Response Teams.

[222] "Montenegro's State Infrastructure Hit by Cyber Attack - Officials," *Reuters*, August 26, 2022, Online edition, https://www.reuters.com/world/europe/montenegros-state-infrastructure-hit-by-cyber-attack-officials-2022-08-26/.

[223] Senior NATO Official, Author Interview on NATO Cyber Rapid Response Teams.

[224] "President of Parliament with French Ambassador," Press Release, Parliament of Montenegro (archived), September 29, 2022, https://www.skupstina.me/en/articles/president-of-parliament-with-french-ambassador#:~:text=The%20President%20took%20the%20opportunity,analysing%20and%20remediating%20the%20consequences.

[225] "President of Parliament with French Ambassador"; "Montenegro's State Infrastructure Hit by Cyber Attack - Officials."

[226] "Letter of Intention by University and Government of Montenegro to Government of France: Montenegro to Be the Place for the Regional Center for Cyber Security and Fight against the Cybercrime," Press Release, Government of Montenegro (archived), March 29, 2022, 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.

structured to achieve one goal – integration of participating state capabilities – at the cost of several other, including crisis response abilities.

A multinational team also complicates liability and information-sharing issues. Montenegro needed to work out any potential legal issues with one actor – France's ANSSI. Information-sharing is more straightforward, too, as it involves only two key players. A CRRT brings with it up to eight different countries and at least as many cybersecurity institutions, each with its own set of resources and prerogatives. While both NATO and the EU CRRT project have worked to establish MOUs to ease cyber intelligence sharing and remediation access, such agreements would likely need to be finessed in the case of a specific situation. Involving multiple countries and stakeholders only complicates and slows the process.

EU CRRTs and NATO RRTs also face significant political hurdles. In the case of NATO, these issues are more pronounced, as any RRT deployment involves an NAC decision and thus automatically invokes all 31 allies. Questions of resource allocation and financial feasibility will surely arise. NAC decisions also often take time and deliberation. In most cases, a state facing a barrage of cyberattacks will look instead to a single decision maker.

The EU CRRTs also involve political complications. Lithuania is clearly interested in adding more members to its project, as it continues to court Czechia and Denmark and lobby observer countries to join as active participants. While expanding the size of the PESCO project has numerous benefits, including adding resources and building stronger ties across participants, it also means adding bureaucratic layers and complexity. CRRT deployments are decided by the CRRT council, which now consists of eight members. Although Lithuania co-chairs the council, it cannot strongarm the group into doing its bidding. And it may not even want to.

There is another additional wrinkle in the rapid response ecosystem: private companies are taking on increasingly larger roles in incident response and remediation. Microsoft has been a key player in Ukraine's defense.[227] The company has also provided support to Montenegro and North Macedonia after the countries suffered cyberattacks.[228] In some cases, private companies have been able to respond more quickly and more flexibly than even single state rapid response teams. They often have intimate details of the troubled state's systems, having built or managed some of its services. The private sector role in crisis mitigation is another open question, and one unlikely to go away in the coming years.

Switzerland should be wary of joining a multinational rapid response team project. The political, financial, and liability issues discussed above would complicate its involvement. If Switzerland wishes to work with EU CRRTs or NATO RRTs, it should focus on the kinds of proactive projects like the deployment in Mozambique. These mission sets fit much more clearly into Switzerland's own vision as a champion of cyber capacity-building efforts.[229]

Switzerland could build its own proactive cybersecurity teams, with the express purpose of training and strengthening a country's cybersecurity and cyber defense *ahead* of a crisis. Such an endeavor could help build goodwill and promote Switzerland's own cybersecurity strengths. Building Swiss teams could also help integrate Swiss cybersecurity institutions – including civilian and military organizations – building stronger connections and identifying expertise. In this way, Switzerland's team building could draw upon the Lithuanian model, but without the complications of integrating multiple countries and their disparate organizations.

In late November 2023, Australia announced the launch of a somewhat similar initiative. The country plans to build rapid cyber assistance teams for use in the Pacific Islands. Australia has responded to cyber crises in the region in the past: in November 2022, the country flew experts to aid Vanuatu after it suffered a massive ransomware attack that incapacitated much of its public sector.[230] This new project, however, is structured for both crisis response and proactive vulnerability mitigation. The government will spend $26 million on the rapid assistance teams and has designated an additional $16.7 million to assess vulnerabilities and test potential solutions.[231] Australia's "Minister for the Pacific Pat Conroy said the rapid response teams would 'build long-

[227] Monica Kaminska, James Shires, and Max Smeets, "Cyber Operations during the 2022 Russian Invasion of Ukraine: Lessons Learned (so Far)" (European Cyber Conflict Research Initiative, July 2022), https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf; Taylor Grossman et al., "The Cyber Dimensions of the Ukraine War," Workshop Report (London: European Cyber Conflict Research Initiative, n.d.).

[228] Senior NATO Official, Author Interview on NATO Cyber Rapid Response Teams.

[229] "Position Paper on Switzerland's Participation in the 2019-2020 UN Open-Ended Working Group on «Developments in the Field of Information and Telecommunications in the Context of International Security» and the 2019-2021 UN Group of Governmental Experts on «Advancing Responsible State Behavior in Cyberspace in the Context of International Security» - January 2020" (Swiss Federal Department of Foreign Affairs, January 2020).

[230] Dubravka Voloder, "Vanuatu Hospital Staff Using Pen and Paper after Cyber Attack That Crippled Public Sector," *ABC News Australia*, November 28, 2022, https://www.abc.net.au/news/2022-11-29/cyber-hack-cripples-vanuatu-public-sector/101705322.

[231] Stephen Dziedzic, "Australia to Deploy Roving Teams of Cyber Experts across Pacific as Online Threats Grow," *ABC News Australia*, November 21, 2023, https://www.abc.net.au/news/2023-11-22/australia-roving-pacific-cyber-experts-online-threats-grow/103135782.

term resilience in the Pacific' and provide critical support."[232]

Australia's new enterprise could be an interesting model for Switzerland. Adding other countries into such an effort – building a Swiss-German or Swiss-French team, for example – could provide greater resources, but could also create the kinds of decision-making and liability complications that arise in the broader multinational teams. Indeed, it seems that Switzerland is best suited to explore forging its own path forward.

[232] "Australia to Form Rapid Cyber Assist Teams for Pacific Islands," *Reuters*, November 22, 2023, https://www.reuters.com/technology/cybersecurity/australia-form-rapid-cyber-assist-teams-pacific-islands-2023-11-22/.

List of Acronyms and Abbreviations

ACO	NATO Allied Command Operations
ANSSI	French National Cybersecurity Agency
APT	Advanced Persistent Threat
CDMB	NATO Cyber Defence Management Board
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team Coordinating Center (first CERT)
CIO	Chief Information Officer
CNMF	US Cyber National Mission Force
CSDP	EU Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
CRRT	EU Cyber Rapid Response Teams
CYCOM	U.S. Cyber Command
CyOC	NATO Cyberspace Operations Centre
EDA	European Defence Agency
EDIDP	European Defence Industry Development Programme
EEAS	European External Action Service
EUPM Moldova	EU Partnership Mission in the Republic of Moldova
EUTM-Moz	European Union Training Mission - Mozambique
FIRST	Forum of Incident Response and Security Teams
FFRDC	Federally Funded Research and Development Center, a private organization sponsored by a US government agency
HR	High Representative of the Union for Foreign Affairs and Security Policy / Vice-President of the European Commission
IPCR	Integrated Political Crisis Response
IRST	Incident Response and Security Teams
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NCI Agency	NATO Communications and Information Agency
NCIRC	NATO Communications and Incident Response Capability
NDPP	NATO Defence Planning Process
NIS	Directive on Security of Network and Information Systems
NIST	National Institute of Standards and Technology
PESCO	EU Permanent Structured Cooperation
POC	EU CRRT Point of Contact
RP	EU CRRT Rotating Participant
RRT	NATO Rapid Reaction Team
SACEUR	NATO Supreme Allied Commander Europe
SEI	Software Engineering Institute, an FFRDC at Carnegie Mellon University
SHAPE	Supreme Headquarters Allied Powers Europe
SSSCIP	Ukrainian State Service of Special Communication and Information Protection
TERENA	Trans-European Research and Education Networking Association
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

Bibliography

"A Progress Report on the Findings of the Future of FIRST Task Force." Santa Clara, California: Future of FIRST Task Force, April 1997. http://web.archive.org/web/19971108090929/http://www.first.org:80/docs/tf97/REPORT.txt.

"Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization." Lisbon, Portugal: NATO, November 19, 2010. https://www.nato.int/cps/en/natohq/topics_82705.htm.

Appathurai, James. "Press Briefing by NATO Spokesman." Presented at the NATO Summit meetings of Heads of State and Government, Kehl, Germany, April 3, 2009. https://www.nato.int/cps/en/natolive/opinions_52841.htm.

Arts, Sophie. "Offense as the New Defense: New Life for NATO's Cyber Policy." *GMF: Strengthening Translatlantic Cooperation* (blog), December 13, 2018.

Author interview with senior PESCO CRRT team official. Interview by Taylor Grossman. Telephone, November 15, 2022.

Benkler, Monika. "Deploying CSDP Missions to Counter Hybrid Threats - EUPM Moldova: First of Its Kind." Tech Pops, August 4, 2023. https://techblog.zif-berlin.org/deploying-csdp-missions-counter-hybrid-threats-eupm-moldova-first-its-kind.

Boeke, Sergei. "National Cyber Crisis Management: Different European Approaches." *Governance* 31 (2018): 449–64.

Boin, Arjen, Madalina Busuioc, and Martijn Groenleer. "Building European Union Capacity to Manage Transboundary Crises: Network or Lead-Agency Model?" *Regulation & Governance* 8 (2014): 418–36.

"Brussels Summit Communiqué." Brussels, Belgium: North Atlantic Treaty Organization, June 14, 2021. https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.

"Brussels Summit Declaration." Brussels, Belgium: North Atlantic Council, July 11, 2018. https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

"Bucharest Summit Declaration." Bucharest, Romania: North Atlantic Council, April 3, 2008. https://www.nato.int/cps/en/natolive/official_texts_8443.htm.

Carnegie Mellon University. "Software Engineering Institute - About the SEI," 2023. https://www.sei.cmu.edu/about/index.cfm.

Cemerka, A. "Ministry of National Defence Preparing Plans for CRRTs to Assist Moldova." *Ministry of National Defence Republic of Lithuania*, September 29, 2022, Online edition. https://kam.lt/en/ministry-of-national-defence-preparing-plans-for-crrts-to-assist-moldova/.

Cerulus, Lauren. "EU to Mobilize Cyber Team to Help Ukraine Fight Russian Cyberattacks." *Politico*, February 21, 2022, Politico Pro Online edition. https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/.

"Chicago Summit Declaration." Chicago, Illinois, United States: North Atlantic Council, May 20, 2012. https://www.nato.int/cps/en/natohq/official_texts_87593.htm?mode=pressrelease.

Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, OJ L 239 § (2017).

"Comprehensive Political Guidance." Riga, Latvia: NATO, November 29, 2006. https://www.nato.int/cps/en/natolive/official_texts_56425.htm.

Council of the EU. "Ukraine: Declaration by the High Representative on Behalf of the European Union on the Cyberattack against Ukraine." Press Release. European Union Council of the European Union, January 14, 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/.

Cyber National Mission Force Public Affairs. "'Committed Partners in Cyberspace': Following Cyberattack, US Conducts First Defensive Hunt Operation in Albania." *U.S. Cyber Command*, March 23, 2023. https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/.

"Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security, Key Roles and Procedures for the CRRTs' Operations, Lessons Learnt from the Cyber Shield / Amber Mist 2018 Exercise." Lithuania: Ministry of National Defence of the Republic of Lithuania, 2018.

"Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security Legal Basis for the CRRTs' Operations." Lithuania: Ministry of National Defence of the Republic of Lithuania, 2018.

Cyberlaw Toolkit, CCDCOE. "Homeland Justice Operations against Albania (2022)," February 2, 2023. https://cyberlaw.ccdcoe.org/wiki/Homeland_Justice_operations_against_Albania_(2022).

Cybil Portal. "Moldova Cybersecurity Rapid Assistance." Project Database. Accessed August 17, 2023. https://cybilportal.org/projects/moldova-cybersecurity-rapid-assistance/.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." *Wired*, August 21, 2007. https://www.wired.com/2007/08/ff-estonia/.

"Defending against Cyber Attacks," 2014. https://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf.

"Defending the Networks: The NATO Policy on Cyber Defence." NATO, 2011. https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf.

Demarest, Colin. "US Sent 'hunt-Forward' Team to Albania in Wake of Iranian Cyberattacks." *C4ISRNet*, March 23, 2023. https://www.c4isrnet.com/cyber/2023/03/23/us-sent-hunt-forward-team-to-albania-in-wake-of-iranian-cyberattacks/#:~:text=Cyber-,US%20sent%20%27hunt%2Dforward%27%20team%20to%20Albania,in%20wake%20of%20Iranian%20cyberattacks&text=WASHINGTON%20%E2%80%94%20U.S.%20cyber%20specialists%20spent,Iranian%20cyberattacks%20on%20government%20systems.

"Deterrence and Defence Posture Review." Chicago, Illinois, United States: NATO, May 20, 2012. https://www.nato.int/cps/en/natohq/official_texts_87597.htm?mode=pressrelease.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=en.

Domingo, Alberto. "NATO Cyberspace Operations." NATO Supreme Allied Commander Transformation presented at the Brief to Maritime Security Regimes Round Table, Norfolk, VA, 2019. http://www.cjoscoe.org/infosite/wp-content/uploads/2019/05/NATO-Cyberspace-Operations.pdf.

DW. "NATO Sees Recent Cyber Attacks on Estonia as Security Issue." May 26, 2007. http://www.dw.com/en/ nato-sees-recent-cyber-attacks-on-estonia-as-security-issue/a-2558579.

Dziedzic, Stephen. "Australia to Deploy Roving Teams of Cyber Experts across Pacific as Online Threats Grow." *ABC News Australia*, November 21, 2023. https://www.abc.net.au/news/2023-11-22/australia-roving-pacific-cyber-experts-online-threats-grow/103135782.

EEAS. "Article 42(7) TEU - The EU's Mutual Assistance Clause," October 6, 2022. https://www.eeas.europa.eu/eeas/article-427-teu-eus-mutual-assistance-clause_en.

EEAS. "EU Partnership Mission in the Republic of Moldova (EUPM)." Official EU Website, 2023. https://www.eeas.europa.eu/eupm-moldova_en?s=410318.

EGA. “Moldova Cybersecurity Rapid Assistance,” 2022. https://ega.ee/project/moldova-cybersecurity-rapid-assistance/#:~:text=The%20European%20Union%20introduced%20Rapid%20Assistance%20Project%20in,aligning%20their%20operations%20with%20the%20EU%20NIS%20Directive.

Elezi, Elona, and Niloofar Gholami. “Albania Blames Iran for Cyberattacks.” *DW*, September 16, 2022. https://www.dw.com/en/albania-once-again-the-target-of-cyberattacks-after-cutting-diplomatic-ties-with-iran-and-expelling-diplomats/a-63146285.

EU Council. Council Decision (CFSP) 2018/340 of 6 March 2018 establishing the list of projects to be developed under PESCO, (CFSP) 2018/340 § (2018). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018D0340.

EU CyberNet. “CCB Projects Mapping.” Database, 2023. https://www.eucybernet.eu/ccb-table/.

“EU Support Package for the Republic of Moldova.” European Commission and European External Action Service, 2023. https://www.eeas.europa.eu/sites/default/files/documents/2023/Support_Package_Moldova-2806.pdf.

European Commission. ANNEX to the Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-sclae cybersecurity incidents and crises, OJ L 239 § (2017). https://eur-lex.europa.eu/eli/reco/2017/1584/oj.

———. “Cyber Defence: EU Boosts Action against Cyber Threats.” Press Release. European Commission, November 10, 2022. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6642.

European Council and Council of the European Union. “Cyber-Attacks: Declaration by the High Representative on Behalf of the European Union Expressing Solidarity with Albania and Concern Following the July Malicious Cyber Activities.” Press Release, September 8, 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/09/08/cyber-attacks-declaration-by-the-high-representative-on-behalf-of-the-european-union-expressing-solidarity-with-albania-and-concern-following-the-july-malicious-cyber-activities/.

European Council and Council of the European Union. “Defence Cooperation: Council Establishes Permanent Structured Cooperation (PESCO), with 25 Member States Participating.” Press Release, December 11, 2017. https://www.consilium.europa.eu/en/press/press-releases/2017/12/11/defence-cooperation-pesco-25-member-states-participating/.

European Defence Agency. “PESCO Projects Adapt and Accelerate Amid Shifting European Security Landscape, EU Report Finds.” July 11, 2023, Online edition. https://eda.europa.eu/news-and-events/news/2023/07/11/pesco-projects-adapt-and-accelerate-amid-shifting-european-security-landscape-eu-report-finds.

European Union. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, OJ C 202 § (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016ME%2FTXT.

Google Translate, trans. “Informal meeting of foreign ministers (Gymnick): Remarks by High Representative / Vice-President Josep Borrell upon arrival.” Press Release. European Union External Action, January 14, 2022. https://www.eeas.europa.eu/eeas/r%C3%A9union-informelle-des-ministres-des-affaires-%C3%A9trang%C3%A8res-gymnich-remarques-du-haut_en?page_lang=en.

Government of Montenegro (archived). “Letter of Intention by University and Government of Montenegro to Government of France: Montenegro to Be the Place for the Regional Center for Cyber Security and Fight against the Cybercrime.” Press Release, March 29, 2022. 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.

Grossman, Taylor, Monica Kaminska, James Shires, and Max Smeets. “The Cyber Dimensions of the Ukraine War.” Workshop Report. London: European Cyber Conflict Research Initiative, n.d.

Healey, Jason, ed. *A Fierce Domain: Conflict in Cyberspace, 1986-2012*. Cyber Conflict Studies Association, 2013.

Herzog, Stephen. “Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.” *Journal of Strategic Studies* 4, no. 2 (Summer 2011): 49–60.

High Representative of the Union for Foreign Affaris and Security Policy. "Joint Communication to the European Parliament and the Council." EU Policy on Cyber Defence. Brussels, Belgium: European Commission and HR, November 10, 2022. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf.

Hoop Scheffer, Jaap de. "Keynote Speech by NATO Secretary General." Presented at the Bucharest Conference, German Marshall Fund, Bucharest, Romania, April 2, 2008. https://www.nato.int/cps/en/natohq/opinions_7608.htm.

"Iranian State Actors Conduct Cyber Operations Against the Government of Albania." Cybersecurity Advisory. CISA, September 23, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a.

"Istanbul Summit Communiqué." Istanbul, Turkey: North Atlantic Treaty Organization, June 28, 2004. https://www.nato.int/docu/pr/2004/p04-096e.htm.

Kaminska, Monica, James Shires, and Max Smeets. "Cyber Operations during the 2022 Russian Invasion of Ukraine: Lessons Learned (so Far)." European Cyber Conflict Research Initiative, July 2022. https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf.

"Key Trends and Statistics of the National Cyber Security Status of Lithuania 2022." Lithuania: Ministry of National Defence, Republic of Lithuania and Cybersecurity National Coordination Centre, Lithuania, 2022. https://kam.lt/wp-content/uploads/2023/06/KEY-TRENDS-AND-STATISTICS-OF-THE-NATIONAL-CYBER-SECURITY-STATUS-2022.pdf.

Krasnec, Tomislav. "Croatia Sends Cyber Warriors to Help Ukraine: This Is Hte First Time This Defense Project Has Been Activated." *Vecernji List*, February 22, 2022. https://www.vecernji.hr/vijesti/hrvatska-salje-cyber-ratnike-u-pomoc-ukrajini-ovo-je-prvi-put-da-je-aktiviran-taj-obrambeni-projekt-1565517.

"Lisbon Summit Declaration." Lisbon, Portugal: North Atlantic Council, November 20, 2010. https://www.nato.int/cps/en/natolive/official_texts_68828.htm.

Lister, Tim. "Secret Document Reveals Russia's 10-Year Plan to Destabilize Moldova." *CNN*, March 18, 2023, online edition. https://edition.cnn.com/2023/03/16/europe/russia-moldova-secret-document-intl-cmd/index.html.

Lithuanian Delegation. "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security." Presented at the Council of the European Union General Secretariat, Brussels, Belgium, March 6, 2019.

Lyngaas, Sean. "Albania Blames Iran for Second Cybreattack since July." *CNN*, n.d., 12 September 2022 edition. https://edition.cnn.com/2022/09/10/politics/albania-cyberattack-iran/index.html.

"Madrid Summit Declaration." Madrid, Spain: North Atlantic Council, June 29, 2022. https://www.nato.int/cps/en/natohq/official_texts_196951.htm.

Miller, Maggie. "Albania Weighed Invoking NATO's Article 5 over Iranian Cyberattack." *Politico*, October 5, 2022. https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347.

Ministry of National Defence, Republic of Lithuania. "EU Cyber Rapid Response Teams to Support Ukraine." Government, February 23, 2022. https://kam.lt/en/eu-cyber-rapid-response-teams-to-support-ukraine/.

Ministry of National Defence Republic of Lithuania. "Lithuanian-Coordinated EU Cyber Rapid Response Teams - Incident Response with the EU and in Support of EU Partners and Military Missions." March 30, 2023. 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/.

Ministry of National Defence Republic of Lithuania. "Lithuanian-Led EU Consortium Develops next-Generation Multifunctional Cyber Toolbox for Defence." May 9, 2022. https://kam.lt/en/lithuanian-led-eu-consortium-develops-next-generation-multifunctional-cyber-toolbox-for-defence/.

Ministry of National Defence Republic of Lithuania. "Progress in Development of Multifunctional Cyber Rapid Response Toolbox at the Ministry of National Defence." June 22, 2022, Online edition. https://kam.lt/en/progress-in-development-of-multifunctional-cyber-rapid-response-toolbox-discussed-at-the-ministry-of-national-defence/.

Ministry of National Defence Republic of Lithuania. "We Have Emerged Stronger from Challenging Situations but We Remain Vigilant, Vice Minister G. M. Tuckute Describes the State of Cybersecurity in Lithuania." June 1, 2023, Online edition. https://kam.lt/en/we-have-emerged-stronger-from-challenging-situations-but-we-remain-vigilant-vice-minister-g-m-tuckute-describes-the-state-of-cybersecurity-in-lithuania/.

"Minutes of the Meeting to Discuss Future Collaborative Activities Between CERTs in Europe." Amsterdam, The Netherlands, September 24, 1999. https://tf-csirt.org/wp-content/uploads/2021/03/planningmeeting-1.pdf.

NATO. "Manfred Boudreaux-Dehmer," November 15, 2021. https://www.nato.int/cps/en/natohq/who_is_who_188597.htm?

NATO. "NATO Reaffirms Support for Albania Following Cyber Attacks." Press Release, September 21, 2022. https://www.nato.int/cps/en/natohq/news_207552.htm?selectedLocale=en.

NATO. "Statement by the North Atlantic Council Concerning the Malicious Cyber Activities against Albania." Press Release, September 8, 2022. https://www.nato.int/cps/en/natohq/official_texts_207156.htm.

NATO CCDCOE. "NATO Summit Updates Cyber Defence Policy." 2014. https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/.

NATO Communications and Information Agency. "About Us." Accessed April 2, 2023. https://www.ncia.nato.int/about-us.html.

"NATO Cyber Defence." Factsheet. NATO, April 2021. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.

NATO Press Release. "Cyber Coalition 2010 Tests NATO's Joint Efforts during Simultaneous Cyber Attacks." November 16, 2010. https://www.nato.int/cps/en/natolive/news_69805.htm.

NATO Press Release. "'Cyber Coalition 2010' to Exercise Collaboration in Cyber Defence." 16 November 20110. https://www.nato.int/cps/en/natohq/news_68205.htm?selectedLocale=en.

"NATO Summit Guide." Warsaw, Poland: NATO, July 8, 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf.

Nielsen, Mads Korsager, and Henrik Moltke. "After massive hacker attacks: Confusion about Danish cyber aid to Ukraine." *DR*, February 20, 2022. 8 April 2023. https://www.dr.dk/nyheder/indland/efter-massive-hackerangreb-forvirring-om-dansk-cyber-hjaelp-til-ukraine.

NL Times. "Ukraine Accepts Dutch Offer of Help against Cyber Attacks." February 22, 2022. https://nltimes.nl/2022/02/22/ukraine-accepts-dutch-offer-help-cyber-attacks.

North Atlantic Treaty Organization. "Cyber Defence," April 4, 2023. https://www.nato.int/cps/en/natohq/topics_78170.htm.

North Atlantic Treaty Organization. "NATO Rapid Reaction Team to Fight Cyber Attack," March 13, 2012. https://www.nato.int/cps/en/natolive/news_85161.htm.

Osborne, James, and Joseph Jarnecki. "Battening Down the Hatches: Moldova's Cyber Defence." *RUSI*, August 10, 2023. https://www.rusi.org/explore-our-research/publications/commentary/battening-down-hatches-moldovas-cyber-defence.

Ottis, Rain. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2008.

Pamment, James, Vladimir Sazonov, Francesca Granelli, Sean Aday, Māris Andžāns, Una Bērziņa-Čerenkova, John-Paul Gravelines, et al. “Hybrid Threats: 2007 Cyber Attacks on Estonia.” Hybrid Threats: A Strategic Communications Perspective. Tallinn, Estonia: NATO Strategic Communications Centre of Excellence, June 6, 2019. https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

Parliament of Montenegro (archived). “President of Parliament with French Ambassador.” Press Release, September 29, 2022. https://www.skupstina.me/en/articles/president-of-parliament-with-french-ambassador#:~:text=The%20President%20took%20the%20opportunity,analysing%20and%20remediating%20the%20consequences.

“Position Paper on Switzerland’s Participation in the 2019-2020 UN Open-Ended Working Group on «Developments in the Field of Information and Telecommunications in the Context of International Security» and the 2019-2021 UN Group of Governmental Experts on «Advancing Responsible State Behavior in Cyberspace in the Context of International Security» - January 2020.” Swiss Federal Department of Foreign Affairs, January 2020.

“Prague Summit Declaration.” Prague, Czech Republic: North Atlantic Treaty Organization, November 21, 2002. https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

Provan, Keith G., and Patrick Kenis. “Modes of Network Governance: Structure, Management, and Effectiveness.” *Journal of Public Administration Research and Theory* 18 (2008): 229–52.

Ranger, Steve. “NATO Updates Cyber Defence Policy as Digital Attacks Become a Standard Part of Conflict.” *ZDNet*, June 30, 2014. https://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/.

Rasmussen, Anders Fogh. “NATO’s Next War - in Cyberspace.” *The Wall Street Journal*, June 3, 2013, Europe Edition edition.

Rehrl, Jochen. “Invoking the EU’s Mutual Assistance Clause. What It Says, What It Means.” *EGMONT Royal Institute for International Relations* (blog), November 20, 2015. https://www.egmontinstitute.be/invoking-the-eus-mutual-assistance-clause-what-it-says-what-it-means/.

Reuters. “Australia to Form Rapid Cyber Assist Teams for Pacific Islands.” November 22, 2023. https://www.reuters.com/technology/cybersecurity/australia-form-rapid-cyber-assist-teams-pacific-islands-2023-11-22/.

Reuters. “Montenegro’s State Infrastructure Hit by Cyber Attack - Officials.” August 26, 2022, Online edition. https://www.reuters.com/world/europe/montenegros-state-infrastructure-hit-by-cyber-attack-officials-2022-08-26/.

Ricks, Thomas E., and Rizwan Ali. “NATO’s Little Noticed but Important New Aggressive Stance on Cyber Weapons.” *Foreign Policy*, December 7, 2017. https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/.

Ridgwell, Henry. “NATO Triggers Rapid Response Force as Russian Forces Advance on Kyiv.” *VOA News*, February 25, 2022. https://www.voanews.com/a/nato-triggers-rapid-response-force-as-russian-forces-advance-on-kyiv-/6459908.html.

“Riga Summit Declaration.” Riga, Latvia: North Atlantic Council, November 29, 2006. https://www.nato.int/docu/pr/2006/p06-150e.htm.

Senior NATO Official. Author Interview on NATO Cyber Rapid Response Teams. Interview by Taylor Grossman. Phone, March 22, 2023.

Shea, Jamie. “How Is NATO Meeting the Challenge of Cyberspace?” *Prism* 7, no. 2 (2017): 19–29.

———. “NATO: Stepping up Its Game in Cyber Defence.” *Cyber Security* 1, no. 2 (May 10, 2017): 165–74.

Slayton, Rebecca, and Brian Clarke. “Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989-2005.” *Technology and Culture* 61, no. 1 (January 2020): 173–206.

———. “Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989-2005.” *Technology and Culture* 61, no. 1 (January 2020): 173–206.

Smith, Brad. “Extending Our Vital Technology Support for Ukraine.” *Microsoft* (blog), November 3, 2022. https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/.

Starks, Tim. “Albania Is the First Known Country to Sever Diplomatic Ties over a Cyberattack.” *The Washington Post*, September 8, 2022, The Cybersecurity 202 edition. https://www.washingtonpost.com/politics/2022/09/08/albania-is-first-known-country-sever-diplomatic-ties-over-cyberattack/.

“Statement Issued by the Heads of State and Government Participating in a Meeting of the North Atlantic Council in Brussels.” Brussels, Belgium: North Atlantic Council, February 22, 2005. https://www.nato.int/docu/pr/2005/p05-022e.htm.

“Strasbourg / Kehl Summit Declaration.” Strasborg, France / Kehl, Germany: North Atlantic Council, April 4, 2009. https://www.nato.int/cps/en/natolive/news_52837.htm.

Thales Cyber Threat Intelligence Team. “2022-2023: A Year of Cyber Conflict in Ukraine.” Thales, March 2023.

“The Istanbul Declaration: Our Security in a New Era.” Istanbul, Turkey: North Atlantic Council, June 28, 2004. https://www.nato.int/docu/pr/2004/p04-097e.htm.

Tidy, Joe. “Ukraine: EU Deploys Cyber Rapid-Response Team.” *BBC*, February 22, 2022, online edition. https://www.bbc.com/news/technology-60484979.

UK Foreign, Commonwealth & Development Office. “UK Boosts Ukraine’s Cyber Defenses with £6 Million Support Package,” November 1, 2022. https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package.

Vasiliauskaite, Egle, and Tadas Sakunas. “Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security, Key Roles and Procedures for the CRRTs’ Operations, Lessons Learnt from the Cyber Shield / Amber Mist 2018 Exercise,” 2019.

———. “Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security, Legal Basis for the CRRTs’ Operations.” Vilnius, Lithuania: Ministry of National Defence of the Republic of Lithuania, January 15, 2019.

———. “Cyber Rapid Response Teams and Mutual Assistance in Cyber Security: Memo for Mutual Assistance in Cyber Security, Legal Basis for the CRRTs’ Operations.” Vilnius, Lithuania: Ministry of National Defence of the Republic of Lithuania, January 15, 2019.

Voloder, Dubravka. “Vanuatu Hospital Staff Using Pen and Paper after Cyber Attack That Crippled Public Sector.” *ABC News Australia*, November 28, 2022. https://www.abc.net.au/news/2022-11-29/cyber-hack-cripples-vanuatu-public-sector/101705322.

“Wales Summit Declaration.” Wales, United Kingdom: North Atlantic Council, September 5, 2014. https://www.nato.int/cps/en/natohq/official_texts_87597.htm?mode=pressrelease.

“Warsaw Summit Communiqué.” Warsaw, Poland: North Atlantic Council, July 8, 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

About the Author

Taylor Grossman was a Senior Researcher in the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zürich. Her research interests include offensive cyber operations, norms development and IHL applicability in cyberspace, organizational politics, and wargaming. She now works as Senior Editor at *Binding Hook*, a media outlet dedicated to technology and security issues. She holds an MPhil in International Relations from the University of Oxford and a BA in Political Science from Stanford University.

CSS
ETH Zürich

The **Center for Security Studies (CSS)** at ETH Zürich is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.