CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn

Innovations in International Cyber Support: Comparing Approaches and Mechanisms for Cyber Capability Support

Joseph Jarnecki
Research Fellow
Royal United Services Institute
London, United Kingdom
jarneckijoseph@gmail.com

Abstract: This paper proposes the concept of international cyber capability support (CCS) to describe a policy area covering the direct provision of cyber security products and services, including the deployment of rapid response teams, with immediate operational impacts intended to advance short-to-medium term objectives. This paper examines illustrative case studies of national cyber crises demonstrating the need for CCS deployment, emerging approaches to providing CCS, and the considerations which should inform how CCS is operationalized.

A recent uptick in large-scale national cyber incidents has demonstrated a clear need for international capabilities to support crisis scenarios. Responses to date have been ad hoc and have exploited crisis conditions to short-circuit normally slow decision-making processes when providing international cyber support. As these incidents become business as usual, formal mechanisms to provide rapid capability responses are being developed. This paper discusses these points, drawing on high-level case studies of Ukraine and Costa Rica.

Capability support outside of crises has also seen a marked increase, such as through personnel deployments as part of Hunt Forward Operations. As countries and international organizations look to establish CCS mechanisms, they need to consider their strategic objectives, implementation, thresholds for deployment and withdrawal, and the remit of their activities. Observing and learning from existing approaches is essential.

Challenges for actors operationalizing CCS mechanisms include aligning activities with partners, creating an enabling and legitimating environment, and monitoring, measuring, and assessing initiatives. From these, this report recommends that actors create a strategic value-case, consider carefully how to integrate multiple stakeholders into CCS mechanisms, and take a comprehensive approach to international cyber support.

Keywords: *international cyber support, cyber capability, cyber capacity building, national cyber crisis*

1. INTRODUCTION

There has been a worrying uptick in national, large-scale cyber incidents in recent years. Montenegro, Costa Rica, Vanuatu, Ukraine, and Albania have all experienced significant effects from cyber attacks; government systems have been crippled and the delivery of critical services delayed or denied.[1] Cyber crisis response, undertaken by countries and big tech companies, has attempted to mitigate the extent and impact of these incidents. To date, this support has been delivered in an agile and ad hoc manner, with minimal formal mechanisms in place. France, the United States, and Microsoft, for example, have reactively deployed teams to several national incidents.[2]

As actors establish formal mechanisms to deliver national cyber crisis responses, they face various challenges, trade-offs, and choices. Who should be providing support and where? What should support entail? How should it be organized? Is support a security, diplomatic, development, or humanitarian matter? And what are the thresholds for deployment and withdrawal? It is also necessary to consider how the provision of capability is operationalized outside of crises, building a cohesive approach to international cyber capability support (CCS).

This paper argues that international CCS mechanisms show promise but have been slow to get off the ground. Moreover, it asserts that emerging frameworks by governments and international organizations should make more use of lessons from recent incidents, particularly those involving multiple implementing actors. Even the most well-resourced actors have limited capabilities to scale up and extend the provision of support, and it remains uncertain whether companies will continue to assist as they have, for example, in Ukraine.

1 Sydney J. Freedberg Jr., 'State Dept Wants "Cyber Assistance Fund" to Aid Allies and Partners Against Hackers', *Breaking Defense*, 10 April 2023; Taylor Grossman, *Cyber Rapid Response Teams Structure, Organization, and Use Cases*, (Zürich: Center for Security Studies ETH Zurich, 2023), 30.

2 Mubariz Zaman, 'Montenegro Thanks France for Assistance Following Cyberattacks', *Diplomatic Insight*, 29 August 2022.

The paper first provides brief case studies of existing ad hoc international cyber support in national cyber crises, focusing on Ukraine and Costa Rica. It then highlights emerging national and international mechanisms for CCS. Finally, the paper identifies significant implications for governments when creating and operationalizing CCS mechanisms, and it outlines priority considerations in a policy-relevant format.

What Is Cyber Capability Support?

This paper uses the term 'cyber capability support' (CCS) to describe a policy area involving the direct provision of products, services, or other cyber security solutions, including rapid crisis response, which have immediate operational impacts that advance short-to-medium-term objectives. For example, CCS includes purchasing licenses, deploying/contracting incident responders, and providing/purchasing actionable cyber threat intelligence (CTI). Activities such as building a security operations centre, conducting a national cyber maturity review, or assessing existing legislation do not fall within this remit; these are more aligned with cyber capacity building (CCB).

CCB is a well-established policy area within international cyber support.[3] Attempts have been made to apply a CCB lens to understand international support responding to national cyber crises and to bring the direct provision of capabilities within CCB frameworks. The desire to not 'reinvent the wheel' is laudable, but CCB frameworks and terminology should not be expected to fit every situation. Policies that aim to create endogenous capacity within recipients should be distinguished from those that provide or deploy capabilities to recipients. The former consists of sustainable, long-term activities, whereas the latter involves operational, responsive, and dynamic support, including in crisis scenarios. Further distinguishing features between CCS and CCB are outlined in Table I.

TABLE I: CCS AND CCB DISTINGUISHING FEATURES

Features	Cyber Capability Support (CCS)	Cyber Capacity Building (CCB)
Timeline	• Rapid deployment, implying dynamic procurement solutions • Typically short-term deployments (<1 year)	• Open competition procurement • Usually mid-to-long-term deployment (>1 year) with limited exceptions
Intended outcome	Achieving targeted and immediate operational objectives to strengthen partner's cyber security resilience and protection in the short-to-medium term, including denying and disrupting adversary activities. Capabilities are provided or purchased to be used by the recipient or are delivered by an implementor.	Creating and supporting endogenous recipient capacity to internally anticipate and respond to cyber risks and threats, including through targeting tactical and strategic outcomes such as improved population cyber hygiene.

3 *See, e.g.*, the 200+ members and partners of the Global Forum for Cyber Expertise, a CCB-focused international organization. 'Members & Partners', GFCE, accessed 4 March 2024, https://thegfce.org/member-and-partner/.

Examples of activities	• Provision of cyber security services, e.g., incident response, remediation • Provision of cyber security products, e.g., firewalls, attack-surface management	• National assessments • Strategy development • Awareness campaigns • Training and education • Limited provision of technical products and services
Examples of policy instruments	• Rapid Response Teams and Mechanisms • Hunt Forward Operations	• Cybersecurity Capacity Maturity Model • National Cyber Risk Assessment • Cyber Defense Exercise with Recurrence
Withdrawal threshold	End of operation, though this is inconsistently defined	End of project or programme

Author-generated

Other attempts to systematize CCS as a policy area have described it as 'cyber defense assistance',[4] 'deployed cyber defence',[5] and 'cybersecurity support deployments'.[6] This paper eschews each of these concepts in an attempt to avoid military language and to posit CCS as a separate but complementary partner to CCB, though it accepts the need to further discuss and align understandings and terminology.

This paper anticipates the critique that CCB is a sufficient frame for all international cyber support and that CCS is not needed. While the sentiment is understandable, it is valuable to discuss and reassess approaches to policy. As international cyber support receives more attention and funding, it is important to demarcate policy areas by type of activity or intended outcome. While CCB and CCS project activities may overlap in places, Table I outlines a sensible set of criteria to divide those building capacities and those providing capabilities. Moreover, the intended outcome of CCB, which is to develop and sustainably build the recipient's own capacities, is not identical to CCS outcomes, which involve providing or purchasing assistance to achieve operational objectives that immediately improve the recipient's cyber security. These differences can be acknowledged without undermining a shared overarching strategic objective: improving and supporting partners' cyber resilience.

This paper focuses primarily on civilian components of CCS and draws exclusively from open-source material. A further study of emerging CCS mechanisms would benefit from primary data-gathering with relevant policymakers.

4 Rattray, Brown, and Moore, 'The Cyber Defense Assistance Imperative Lessons'.

5 Nick Beecroft and Toby Gilmore, 'The Advantages of "Hunt Forward" Extend Beyond the Hunt', *BAE Systems Digital Intelligence*, 2023.

6 Julia Schuetze and Eglė Daukšienė, 'Cybersecurity Support Deployments: An Emerging Cooperative Approach', Stiftung Neue Verantwortung, 15 June 2023, https://www.stiftung-nv.de/en/publication/cybersecurity-support-deployments.

2. TWO CASE STUDIES: UKRAINE AND COSTA RICA

This section addresses two recent case studies of rapid international cyber crisis response to demonstrate the increasing salience of and need for these activities, as well as their use of ad hoc processes.

A. Case Study: Sustained Russian Cyber Campaign against Ukraine

Russian cyber operations against Ukraine began scaling up before the invasion in February 2022 and have continued throughout the war. Reports from that period indicate a shift from sophisticated and long-term cyber operations to intelligence gathering and less sophisticated destructive tactics.[7] Significant effects have been observed on Ukrainian critical infrastructure, such as the 2024 attack on the telecom company Kyivstar.[8]

Before the invasion, several actors were conducting CCB in Ukraine. These included the European Union, the US, Estonia, France, the United Kingdom, and Germany, focused on areas such as cybercrime, cyber hygiene, and awareness building.[9] As war became more likely, some actors undertook CCS, deploying targeted services to improve Ukrainian systems resilience. Public information on these activities is limited; however, the US Cyber Command's (USCYBERCOM) Hunt Forward Operation (HFO) has been disclosed publicly. An HFO involves deployed personnel hunting for threats on partner networks alongside local counterparts.[10] The mission to Ukraine (December 2021 to February 2022), which was praised by a senior Ukrainian cyber security official, included the discovery of ninety malware samples.[11]

Once the war began, cyber support became one part of a broader assistance to Ukraine. Limited information is available on support to the Ukrainian Defence Ministry and armed forces; a notable exception is the IT Coalition, which is part of the Ramstein format.[12]

7 *See, e.g.*, 'Cyber Conflict in the Russia-Ukraine War', Carnegie Endowment, accessed 3 January 2024, https://carnegieendowment.org/programs/technology/cyberconflictintherussiaukrainewar/; Google TAG and Mandiant, 'Fog of War', Google, February 2023, https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

8 Tom Balmforth, 'Exclusive: Russian Hackers Were Inside Ukraine Telecoms Giant for Months', *Reuters*, 5 January 2024, https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

9 For CBB project details, *see* Cybil Portal, 'Projects', Cybil, accessed 4 January 2024, https://cybilportal.org/projects-advanced/?_sft_country=ukraine&_sfm_status_project=Finished.

10 US Cyber Command Public Affairs, 'CYBER 101: Hunt Forward Operations', US Cyber Command, 15 November 2022, https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/.

11 Dina Temple-Raston et al., 'Exclusive: Ukraine Says Joint Mission with US Derailed Moscow's Cyberattacks', *Record*, 18 October 2023, https://therecord.media/ukraine-hunt-forward-teams-us-cyber-command.

12 European Pravda, 'Ramstein Format Meeting: 10 IT Coalition Countries Sign 6-Year Cooperation Agreement', *Ukrainska Pravda*, 14 February 2024, https://www.pravda.com.ua/eng/news/2024/02/14/7441891/.

There is more open-source information on non-military CCS activities by countries and private companies. Among foreign governments, the UK moved first to establish the Ukraine Cyber Programme (UCP) shortly after the invasion and has since welcomed funding from other international donors to expand activities.[13] The UCP has utilized cyber security providers to supply incident response (IR), DDoS (distributed denial-of-service) protection, firewalls, and forensic capabilities.[14] Germany has sent cyber security hardware as humanitarian aid to Ukraine's energy sector.[15] Microsoft, Google, and other private companies have provided various licenses, tools, and technical assistance.[16] Other international actors have also conducted CCS, with the general approach being ad hoc cyber assistance to Ukraine.[17]

Efforts to coordinate CCS to Ukraine began in the private sector with the Cyber Defence Assistance Collaborative (CDAC).[18] A volunteer group of cyber security and technology companies established in March 2022, the CDAC minimized the risk of duplication and streamlined assistance.[19] Governments have been slower to establish similar structures, with the Tallinn Mechanism announced in December 2023 and the Ramstein format IT Coalition formalized in February 2024.[20] The Tallinn Mechanism's three chronological lines of effort – 'short (Support), medium (Build) and long-term (Sustain)' – imply that CCS-type activities are covered in addition to CCB, as does its commitment to 'maintain and strengthen' Ukrainian cyber resilience.[21] If this interpretation is correct, the Tallinn Mechanism coordinates a hybrid of CCS and CCB activities.

This paper considers CCS to Ukraine to include rapidly deployed activities taken to directly provide cyber security products or services with immediate operational impacts on advance short-to-medium-term objectives. For example, USCYBERCOM's HFO deployed personnel to provide threat hunting services, and the UCP purchases products and services for Ukrainian systems resilience. By contrast, CCB initiatives

13 Prime Minister's Office, 'UK to Give Ukraine Major Boost to Mount Counteroffensive', GOV.UK, 18 June 2023, https://www.gov.uk/government/news/uk-to-give-ukraine-major-boost-to-mount-counteroffensive.

14 FCDO, 'UK Boosts Ukraine's Cyber Defences with £6 Million Support Package', GOV.UK, 1 November 2022, https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package.

15 Cybil Portal, 'Supporting Ukraine's Cybersecurity Agency with Hardware', *Cybil*, accessed 4 January 2024, https://cybilportal.org/projects/supporting-to-ukraines-cybersecurity-agency-with-hardware/.

16 Nick Beecroft, 'Evaluating the International Support to Ukrainian Cyber Defense', Carnegie Endowment, 3 November 2022, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322.

17 'Tallinn Mechanism', Estonian Ministry of Foreign Affairs, https://www.vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/tallinn-mechanism.

18 Greg Rattray, Jeff Brown, and Robert T. Moore, 'The Cyber Defense Assistance Imperative Lessons from Ukraine', Aspen Institute, February 2023, https://creativecommons.org/licenses/ by-nc/4.0/.

19 Rattray, Brown, and Moore, 'The Cyber Defense Assistance Imperative Lessons'.

20 Other parties to the mechanism include Canada, France, Germany, the UK, Netherlands, Poland, Sweden, Ukraine, and the US.

21 'Tallinn Mechanism', Government of Canada, last modified 19 December 2023, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/tallinn-mechanism-mecanisme-tallinn.aspx?lang=eng.

such as USAID's 'Cybersecurity for Critical Infrastructure' project, while significant and substantial, have long-term, primarily strategic objectives to develop Ukraine's own capacities. Grouping both sets of activities – CCB and CCS – within a single policy framework that necessitates similar approaches to processes such as funding and procurement makes it difficult to respond appropriately to donor objectives and recipient needs.

B. Case Study: Ransomware Attacks on Costa Rica

'We are determined to overthrow the government by means of a cyber attack …' – Conti, a ransomware group[22]

In spring 2022, Costa Rica experienced a series of cyber attacks which led the president to declare a national emergency and announce that the country was 'at war'.[23] Beginning on 17 April, the ransomware group Conti launched attacks in rapid succession, impacting twenty-nine government institutions.[24] These abated in early May, but new attacks, now by the Hive ransomware group, started on 31 May, targeting the Costa Rican Social Security Fund.[25]

The campaigns by Conti and Hive disrupted the delivery of critical services. Ministry of Finance digital systems to declare taxes and customs were shut down. So were some Social Security Fund services, which affected an estimated 4,871 medical appointments in the initial twenty-four hours.[26] Response costs for the government were over US$24 million as of June 2022, and economic losses from disruptions to trade have been estimated at US$38 million per day.[27]

In one of the first actions taken in response to the attacks, the government of Costa Rica asked Spain, the US, and Israel for advice and support.[28] Spain, which had a pre-existing agreement with Costa Rica, sent 100,000 licenses for a counter-ransomware tool and deployed a government technical team. Israel, which had cemented bilateral cyber relations with a memorandum of understanding (MoU), provided CTI.[29] The US deployed an FBI technical team and offered a US$10 million reward for information

22 Jonathan Grief, 'Ransomware Gang Threatens to "Overthrow" New Costa Rica Government, Raises Demand to $20 Million', *Record*, 16 May 2022, https://therecord.media/ransomware-gang-threatens-to-overthrow-new-costa-rica-government-raises-demand-to-20-million.

23 'President Rodrigo Chaves says Costa Rica is at war with Conti hackers', BBC News, 18 May 2022, https://www.bbc.com/news/technology-61323402.

24 Eugenia Lostri and Georgia Wood, 'The Role of International Assistance in Cyber Incident Response', *Lawfare*, 30 March 2023, https://www.lawfaremedia.org/article/role-international-assistance-cyber-incident-response.

25 Jonathan Grieg, 'Costa Rican Social Security Fund Hit with Ransomware Attack', *Record*, 31 May 2022, https://therecord.media/costa-rican-social-security-fund-hit-with-ransomware-attack.

26 Andrea More, 'CCSS report afectación de 4.871 usarios en 80 establecimientos de salud, tras hackeo a sistemas informáticos', *Delfino*, 1 June 2022, https://delfino.cr/2022/06/ccss-reporto-afectacion-de-4-871-usuarios-en-80-establecimientos-de-salud-tras-hackeo-a-sistemas-informaticos.

27 Lostri and Wood, 'The Role of International Assistance'.

28 Ibid.

29 Ibid.

on Conti's leadership.[30] Microsoft and Cisco supplied free tools, and Microsoft provided unspecified additional technical assistance.[31] This report argues that these support efforts fall under CCS.

To the author's knowledge, no actor providing CCS to Costa Rica had specific policies in place to conduct that kind of activity. Moreover, there was no prior decision-making process to determine that – along with the private sector – the US, Spain, and Israel were appropriate and legitimate responders. Nor were there thresholds, at least publicly, in place to determine what triggered a request for assistance. Presumably, once they were engaged, supporting actors deconflicted their activities, but this is not certain. Equally unclear was how they determined when to withdraw support – the US continued to launch new initiatives into 2023, though these focused on building capacity.[32] Did the US deliberately transition its activities from providing capability to building capacity in Costa Rica?

CCS to Costa Rica was welcomed and had an impact. President Chaves has stated he has '25 million reasons to be grateful' for the cyber security support.[33] A high-profile attack has also motivated other Latin American countries, with many subsequently creating national cyber security strategies – from twelve in 2020 to over twenty by 2024.[34]

While individual national preparations are welcome, measures to formalize international CCS are moving more slowly. A warning from Conti, released during its attacks on Costa Rica, should encourage these processes: 'The Costa Rica scenario is a beta version of a global cyber attack on an entire country'.[35]

30 Ned Price, 'Reward Offers for Information to Bring Conti Ransomware Varient Co-Conspirators to Justice', US Department of State, Press Statement, 6 May 2022, https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/.

31 Lostri and Wood, 'The Role of International Assistance'.

32 'United States Announces $25 Million to Strengthen Costa Rica's Cybersecurity', US Embassy in Costa Rica, 29 March 2023, https://cr.usembassy.gov/united-states-announces-25-million-to-strengthen-costa-ricas-cybersecurity/.

33 Luke O'Grady, 'Event Recap: A Conversation with Rodrigo Chaves Robles, President of Costa Rica', Center for Cybersecurity Policy and Law, 6 November 2023, https://www.centerforcybersecuritypolicy.org/insights-and-research/event-recap-a-conversation-with-rodrigo-chaves-robles-president-of-costa-rica.

34 Cecilia Tornaghi, 'The Dramatic Cyberattack that Put Latin America on Alert', *Americas Quarterly*, 25 July 2023.

35 VenariX (@_venarix_), '#Conti's latest update on the cyberattack…', X, 20 April 2022, https://twitter.com/_venarix_/status/1516569937418113025.

3. EMERGING APPROACHES

This section outlines and considers existing, emerging, or proposed mechanisms and programmes to coordinate and conduct CCS. Private-sector-led initiatives such as the CDAC are excluded in the interest of brevity. This section supports the argument that existing and emerging CCS mechanisms are making good progress but that there are diverse issues to consider and best practices to integrate.

Table II provides an overview of CCS mechanisms and programmes for which there is open-source information.

TABLE II: OVERVIEW OF CCS MECHANISMS AND PROGRAMMES

Entity	Mechanism	Description
European Union (EU)	Cyber Reserve[36]	• Proposal under the EU Cyber Solidarity Act • Private IR services deployable at the request of EU members or organizations • Response to significant or large-scale cyber security incidents • Funding for whole proposed Act (including other provisions) is €1.1 billion
US State Department	Cyberspace, Digital connectivity, and related Technology (CDT)[37]	• State Department fund, including CCS such as emergency assistance capacities • Deployed at the discretion of the secretary of state • Created under the 2023–2024 Department of State Authorization Act • US$150 million for five-year period from 1 October 2023
Ukraine Defence Contact Group (UDCG)	IT Coalition[38]	• Ten-country initiative within the Ramstein Format coordinating defence support to Ukraine • Established with six-year commitment to deliver secure and resilient IT infrastructure for Ukrainian defence forces • Funding unclear, with some individual members announcing contributions, e.g., €10 million each from both Luxembourg and the Netherlands
UK Foreign Commonwealth & Development Office (FCDO)	Ukraine Cyber Programme (UCP)[39]	• Direct programme to provide CCS to Ukraine, supporting networks against Russian attacks • Launched February–March 2022 • Procurement of private providers by FCDO • £7.1 million programme expenditure with a further up to £25 million of multi-country funding committed from June 2023 – potential £9 million from allies

36 36 "The EU Cyber Solidarity Act', European Commission, updated 6 March 2024, https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

37 "Text - S.2043 - 118th Congress (2023-2024): Department of State Authorization Act of 2023', Congress.gov, 22 August 2023, https://www.congress.gov/bill/118th-congress/senate-bill/2043/text/is.

38 'Increased Support from Partners, Capabilities Coalition and IT Coalition - Outcomes of the 15th Ramstein Meeting', Ministry of Defence of Ukraine, Government Portal, 19 September 2023, https://www.kmu.gov.ua/en/news/bilshe-pidtrymky-vid-partneriv-capabilities-coalition-it-koalitsiia-pidsumky-15-oi-zustrichi-u-formati-ramshtain; Viktoria Stepanenko, New Air Defense Coalition and Military Aid Agreed at Latest Ramstein Meeting', *Kyiv Post*, 24 November 2023, https://www.kyivpost.com/post/24566; 'Netherlands Joins IT Coalition to Support Ukraine and Contributes Over $10 mn', Army Recognition, 29 January 2024, https://armyrecognition.com/ukraine_-_russia_conflict_war_2022/netherlands_joins_it_coalition_to_support_ukraine_and_contributes_over_$_10_mn.html?utm_content=cmp-true.

39 Prime Minister's Office, 'UK to give Ukraine Major Boost'.

USCYBERCOM	HFO[40]	• Rooted in 2018 Department of Defense Cyber Strategy doctrine of defend forward and persistent engagement • Involving the deployment of USCYBERCOM operators to hunt for threats alongside host nation counterparts • Over 50 deployments to 24 countries[41]
EU Permanent Structured Cooperation (PESCO)	Cyber Rapid Response Teams (CRRT)[42]	• Multi-country/pooled IR capability; nine members as of September 2023[43] • Launched in February 2018 • Provision of emergency response, confidence-building, and training to partners who request it • Teams composed of government experts • Deployments to Ukraine, Mozambique, and Moldova • Operations funded jointly by providers and recipients
Counter Ransomware Initiative (CRI)	CRI Incident Response (CRI-IR)[44]	• Fifty country members committed, under 2023 joint statement, to assist in IR if government or lifeline sectors are hit by ransomware • Few details available
Australia Department of Foreign Affairs & Trade (DFAT)	Regional Cyber Crisis Response Team (R-CCRT)[45]	• Mechanism to provide CCS • Limited to Pacific and Southeast Asian countries experiencing severe cyber incidents • Coordinated by Australia's Cyber Ambassador within DFAT • Funding around A$26–A$43 million
Foreign ministries: US, Canada, Denmark, Estonia, France, Germany, the Netherlands, Poland, Sweden, UK	Tallinn Mechanism[46]	• Coordinates and facilitates 10 countries' civilian international cyber support (CCS & CCB) to Ukraine • Launched in December 2023 • NGO and private sector involvement stated but not detailed • Presumably no funding distribution function, just deconfliction and coordination among members
North Atlantic Treaty Organization (NATO)	Virtual Cyber Incident Response Capability (VCISC)	• Country members provide assistance for post-incident mitigation • Launched at Vilnius Summit July 2023 • Few operational details available

Author-generated

A. Organization

Understanding how mechanisms are organized is key to understanding their proliferation, as well as their intended and actual abilities. Australia's R-CCRT and the US's CDT and HFOs are national mechanisms, whereas the EU's CRRT and

40 US Cyber Command Public Affairs, 'CYBER 101: Hunt Forward Operations', US Cyber Command, 15 November 2022, https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/.

41 Patty Nieberg, '"Hunt Forward" Cyber Teams Have Deployed to 24 Countries, Including Ukraine', *Task & Purpose*, 28 September 2023, https://taskandpurpose.com/news/cyber-command-security-hunt-forward/.

42 PESCO, 'Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRT)', PESCO Projects, accessed 11 January 2024, https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/.

43 Belgium, Denmark, Estonia, Croatia, Lithuania, Poland, Netherlands, Romania, and Slovenia.

44 'International Counter Ransomware Initiative 2023 Joint Statement', White House, 1 November 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/.

45 Australian Government, *Australian Cyber Security Strategy 2023-2030* (Canberra: Australian Government Department of Home Affairs, 2023).

46 "Tallinn Mechanism', Estonian Ministry of Foreign Affairs, 21 December 2023, https://www.vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy/tallinn-mechanism.

Cyber Reserve, NATO's VCISC, the UDCG's IT Coalition, the Tallinn Mechanism, and the CRI-IR are multinational. The UK's UCP began as a national programme but ostensibly became a multi-country-funded mechanism (see Table II).

1) Multinational

The EU's CRRT is a limited member mechanism coordinated by permanent and rotating co-chairs; one co-chair, Lithuania, is permanent. The CRRT's response teams are supposed to consist of experts from multiple members, though how often this is actually achieved is uncertain.[47] Both the IT Coalition and the Tallinn Mechanism are ten-country initiatives, and the latter states that it also involves tech companies and NGOs. The former is headed by Estonia and Luxembourg, and the latter has a front office in Kyiv run by Estonia and a back office in Poland.

The full scope of the EU Cyber Reserve remains unclear, largely because it is in development, though initial indications are that it will procure assistance, funded by the EU, from a pool of private incident responders. While details of its projected funding are unclear, it is likely over €100 million.[48]

The UK's UCP was launched as a national initiative, which, in June 2023, welcomed additional funding from international partners, thus becoming multinational.

The CRI-IR and NATO's VCISC are at present too opaque to draw conclusions about their organization.

2) National

The US CDT, which operates alongside USCYBERCOM HFOs, deployments by the FBI, and CCB delivered by USAID, is part of an increasingly comprehensive approach the country is taking to international cyber support. Acknowledging this, the authorization of funds for the CDT is contingent upon a 'review of emergency assistance capacity' by the secretary of state within a year.[49] Australia's R-CCRT aligns with the country's stance that cyber response can be a humanitarian activity and builds on the regional focus of its existing CCB.[50] The significant funding that the US and Australian governments have allocated to new CCS mechanisms indicates their increasing focus on the policy area (see Table II).

B. Remit

Policymakers coordinating mechanisms and programmes in Table II have sought to elaborate clear remits to avoid mission creep.

47 Grossman, 'Cyber Rapid Response Teams'.

48 'The EU Cyber Solidarity Act', European Commission, updated 6 March 2024, https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

49 Congress.gov, 'Text - S.2043'.

50 Cybil Portal, 'Projects', Cybil, accessed 10 January 2024, https://cybilportal.org/projects-advanced/?_sft_funder=australia.

The listed initiatives' remits can be grouped across membership, geography, and priority/opportunity criteria (see Table III). The CRI-IR, NATO's VCISC, and the EU's Cyber Reserve provide membership-based support, which may be mediated through a multinational body. The UCP, the Tallinn Mechanism, and the IT Coalition, as well as Australia's R-CCRT, have geographical focuses – Ukraine for the first three and the Pacific Islands and Southeast Asia for the last one. Finally, the US CDT and HFOs have looser remits, each determined by government priorities. For example, the CDT states that its activities are intended to 'advance a stable and secure cyberspace' and 'support and reinforce democratic values and human rights'.[51] The CRRT ostensibly focuses on EU member states and organizations, but in practice it has, for example, supported Mozambique and Moldova.

TABLE III: OVERVIEW OF MECHANISM REMITS

Remits		
Membership	Geography	Priority/Opportunity
• CRI-IR • VCISC • Cyber Reserve	• UCP • Tallinn Mechanism • IT Coalition • R-CCRT	• CDT • HFO • CRRT

Author-generated

C. Thresholds

Factors that shape the thresholds for deployment of a given mechanism include the scale of incidents, types of attack, and political decision-making.

A significant, large-scale crisis or emergency or a severe incident is the threshold for response for NATO's VCISC, the EU's Cyber Reserve and CRRT, Australia's R-CCRT, and the CRI-IR. However, none of these mechanisms define precisely what this means. Given that they are programmes, not reproducible mechanisms, the IT Coalition, UCP, and the Tallinn Mechanism do not provide thresholds for further deployment, but each stemmed from Russia's large-scale cyberattacks on Ukraine.

The threshold for CRI-IR activation is limited to ransomware attacks that hit government or lifeline sectors.

US HFOs and the CDT have no publicly disclosed thresholds for deployment. Instead, they activate at the discretion of USCYBERCOM and the secretary of state, respectively.

51 Congress.gov, 'Text - S.2043'.

Thresholds for withdrawal are less elaborated and highly sensitive; publicly defining a limit to support may encourage adversaries or undermine relationships with partners. As such, all mechanisms but the IT Coalition have avoided setting hard limits. The IT Coalition has set a six-year horizon on its activities; this might be a response to domestic pressures, though no reason has been stated publicly.

D. Private Sector Involvement

The mechanisms in Table II have considered how to include private companies; a high-level overview is provided in Table IV.

One approach, adopted by the US's CDT and the UK's UCP, is to use private sector companies as implementing partners. Under this approach, companies operationalize CCS. The EU Cyber Reserve has similarly indicated it would use private-sector implementation and would maintain a list of trusted providers. The Tallinn Mechanism goes further by referring to tech companies and NGOs in donor countries as mechanism participants, though it does not clarify what this entails. To the author's knowledge, US HFOs have never integrated private sector provision. According to Taylor Grossman, the EU's CRRT had intended to do so but has been hampered by classification and liability issues.[52]

Australia's R-CCRT commits to drawing on industry experience. The author's assumption is that this involves contracting private sector implementation, though this has not been clarified publicly. The capabilities which the IT Coalition and NATO's VCISC commit to providing – IT infrastructure and national mitigation – imply private sector delivery, though, again, this has not been confirmed. Lastly, the CRI has sought to incorporate the private sector in its wider initiatives; however, their role in the CRI-IR commitment has not been discussed publicly.

TABLE IV: ROLE OF PRIVATE SECTOR

Private Sector Involvement			
Implementation Partners	Mechanism Partners	Not Involved	Unclear
• CDT • UCP	• Tallinn Mechanism • Cyber Reserve	• HFO • CRRT	• VCISC • R-CCRT • CRI-IR • IT Coalition

Author-generated

52 Grossman, 'Cyber Rapid Response Teams', 18.

4. OPERATIONALIZING CCS

This section outlines thematic issues for CCS provision and priority considerations for mechanisms. These are summarized by single words or phrases to promote their adoption by policymakers.

This section supports the argument that emerging CCS mechanisms are promising and that key considerations are coming to the fore. Actors intending to create or improve their CCS offering should learn from the existing efforts of like-minded partners.

A. Alignment

Deconfliction. Points of duplication exist among mechanisms outlined in Table II. Papua New Guinea, for example, is a CRI member and is covered by Australia's R-CCRT. If Papua New Guinea suffers a severe incident, who would respond? As more mechanisms emerge, especially those without geographical limitations, there is a risk of further duplication. While efforts to deconflict mechanisms seem desirable, having overlapping coverage could mitigate the risk of overloading one mechanism. Managing these overlaps, however, will be difficult. Actors want to respond to the most severe and strategically significant incidents; thus, they might be incentivized to compete to provide capability in some cases but under-supply in others. This is further complicated by the involvement of big tech in CCS; for example, Microsoft has responded to national incidents in Costa Rica, Ukraine, Albania, and elsewhere.[53] The provision of CCS by diverse, multi-stakeholder actors creates a need to understand incentives and to conduct regular communication, coordination, and deconfliction. Efforts to coordinate diverse multi-stakeholder activities will inevitably encounter significant difficulties, as demonstrated by CCB, but this should not dissuade actors from making the attempt.

In addition to managing duplication among stakeholders, actors operationalizing CCS need to consider how to structure their activities around ongoing CCB. This paper advocates that CCS covers activities to provide capability, especially in anticipation of, during, and immediately after significant incidents. At any stage of CCS intervention, there could be previous, ongoing, or planned CCB. While CCS and CCB have distinct intended outcomes, they should not be conducted in isolation and should be joined up where possible. Actors offering broad international cyber support face a challenge in taking a comprehensive approach and ensuring that CCS and CCB activities are complementary.

53 Brad Smith, 'Defending Ukraine: Early Lessons from the Cyber War', Microsoft, 22 June 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/; Microsoft Threat Intelligence, 'Microsoft Investigates Iranian Attacks Against the Albanian Government', Microsoft, 8 September 2022, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/.

Cohesion. Actors conducting CCS should consider how to work with likeminded partners to ensure their efforts are cohesive and complementary. Multi-member CCS mechanisms pool resources, encourage economies of scale, and can streamline processes such as information sharing and requests for assistance. They also require collaborative objective setting; for instance, the CRI-IR has the strategic objective of mitigating the effects of ransomware. Setting and sticking to these objectives could prove difficult, as participants hold differing views. For instance, some participants argue for lower thresholds to provide CCS, while others prioritize attribution over remediation, and assembling joint teams can prove intractable, as gaps in trust prevent information sharing. These considerations for multi-member mechanisms are reproduced to some extent within the governments that run national mechanisms. Achieving cohesion is easier said than done and is it not necessarily always possible or desirable.

B. Enabling Environment

What can be done. Mechanisms, whether national or multinational, require that actors or groups split up certain competencies across people, process, and technology.

- Implementing personnel can be direct employees of funders, as with USCYBERCOM's HFOs, or contracted. Required personnel are not just technical individuals deploying tools and services; CCS projects also need strong project and stakeholder management. To sustain a standing mechanism, donors may require a secretariat, as the Tallinn Mechanism shows (see Section 3.A).
- Clear and targeted processes are important for the success of CCS mechanisms. This is especially the case for rapid response, where internal processes could activate teams that are on standby 24/7. Alternatively, if private sector deployment is leveraged, a rapid response capability could be serviced by a retainer arrangement, where a company is paid a fee to ensure that responders are on hand whenever necessary.
- Technological resources to provide CCS can be held or created by actors directly or acquired from industry, such as the UCP purchasing forensic capabilities.[54]

Given that mechanisms may need to address incidents of increasing complexity, and multiple incidents simultaneously, they need to be scalable. This paper suggests that a sufficient capacity to scale up CCS is unlikely to be achieved outside the most well-resourced countries but is more feasible in a multi-country mechanism. A more realistic approach, however, may be to design a multi-stakeholder mechanism that integrates private sector delivery, though this raises questions about whether companies can legitimately provide this support, whether principals and shareholders

54 FCDO, 'UK boosts Ukraine's Cyber Defences'.

believe it is worthwhile, and whether companies share values and objectives with states and international organizations. On the other hand, are CCS mechanisms possible without the private sector? While national in-house CCS mechanisms may present fewer challenges in setting strategic direction, integrating multi-stakeholder implementing partners is likely essential to achieving comprehensive coverage.

Mechanisms which leverage private sector delivery, especially for rapid response, depend on effective funding and procurement processes. Actors should consider whether their existing processes are appropriate – for example, whether sufficient funding is eligible for capability provision and whether procurement processes accommodate cyber security providers with minimal experience in other international support activities. Hopefully, donors and researchers will conduct further analyses of funding and procurement issues.

What should be done. Actors operationalizing CCS need to consider their legitimacy to act. National and international law is decisive in determining legitimacy. For example, some countries' constitutions prohibit or limit foreign security assistance, and international law presents considerations related to requests for assistance.[55] Actors providing CCS in limited geographical or country contexts could account for these issues by pre-agreeing MoUs with partners, though these require extended and complex negotiations. For less targeted mechanisms, substantial effort is required to anticipate legal issues such as data-sharing, classifications, procurement, and funding rules.

C. Monitoring and Measurement

Justification. The perceived success of CCS mechanisms depends on how they are monitored, measured, and evaluated. Donors need to understand the value-case of activities and whether their implementation provides a sufficient return on investment. None of the actors running the mechanisms outlined in Table II have released information on these considerations, but similar thinking on CCB indicates it is a consideration.[56] Part of assessing the value-case involves actors deciding strategic priorities for CCS, such as humanitarian, security, commercial, or influence priorities. For example, NATO's VCISC is focused on national mitigation among allies; Australia's R-CCRT supports regional partners, presumably in the interest of building influence; and the US CDT integrates some commercial priorities. Furthermore, those determining value should expect questions about moral hazard: does the creation or provision of CCS disincentivize national cyber security preparation to avoid large-

55 Net Politics, 'How Japan's Pacifist Constitution Shapes its Approach to Cyberspace', Council on Foreign Relations, 23 May 2018, https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace; Louise Marie-Hurel, 'Decoding Emerging Threats: Ransomware and the Prevention of Future Cyber Crises', RUSI, 11 September 2023, https://rusi.org/explore-our-research/publications/conference-reports/decoding-emerging-threats-ransomware-and-prevention-future-cyber-crises.

56 Faisal Hameed et al., 'Analysing Trends and Success Factors of International Cybersecurity Capacity-Building Initiatives', in *Twelfth International Conference on Emerging Security Information, Systems and Technologies*, 2018.

scale incidents? From this question, some actors may decide to impose conditions on assistance, though this could impact relationships with partners. Worse still, will the existence of these mechanisms incentivize adversaries to conduct attacks triggering responses? Could the resource strain of providing CCS divert resources better spent elsewhere?

Challenge and response. Monitoring and measuring policy mechanisms is a persistent challenge. To monitor mechanisms, implementers and funders need oversight and access to data on the impacts of implementation as well as an assessment framework. While monitoring and measuring is not easy, this paper asserts that it is possible to do so for CCS while acknowledging that some indicators (e.g., number of attacks) are clearer than others (e.g., deterring adversaries).

The data-rich nature of many CCS activities provides a valuable opportunity to monitor knowable or calculable impacts. For example, providing a cloud-based malware analysis tool could involve implementers receiving information on recipient tool usage as part of product improvement cycles. Similarly, IR services will involve implementers collecting data such as malware samples. If relevant calculable information was captured and submitted as part of activity assessment frameworks, CCS projects could be effectively measured and evaluated. Gathering and exfiltrating data, however, may be unacceptable to recipients who are concerned about unauthorized access by malicious actors.

Assessing CCS impacts also relies on subjective or qualitative judgements based on smaller or more opaque data sets. For example, assessing CCS activities intended to deny or deter adversaries relies on an understanding of adversary perceptions and reactions. The need to make this judgement is nothing new; actors developing CCS mechanisms should consider assessment approaches from existing foreign, defence, and security policy.

D. Considerations for CCS Mechanisms

Establishing and maintaining CCS mechanisms is complex. This paper argues that the most urgent points for actors to consider are creating a measurable strategic value-case, determining multi-stakeholder involvement in CCS, and creating a comprehensive approach to international cyber support.

A measurable strategic value-case. As with other international support activities, CCS does not have a single strategic value-case across donors. Currently, mechanisms' strategic objectives include development and humanitarian support, security, and diplomacy. Strategic objectives shape actors' provision of CCS, as they influence factors such as potential partners, eligible funding, responsible internal agencies,

ability to scale, and thresholds for provision and withdrawal. Actors' ability to measure and assess CCS activities with reference to these strategic objectives will be decisive in determining whether mechanisms are maintained in the medium term. While CCS mechanisms now seem to be proliferating rapidly, there is no guarantee that this will continue or that they will be beneficial.

Multi-stakeholderism. This paper has focused on CCS provided by countries and international organizations and has largely considered the private sector as an operational delivery partner. The CDAC in Ukraine and the provision of CCS-type activities in multiple national cyber incidents by companies such as Microsoft, however, demonstrate that private sector actors are independent strategic CCS players.[57] In this context, national and international CCS mechanisms must consider how, when, and in what way they engage with the private sector. The Tallinn Mechanism, for example, has ostensibly integrated the private sector, but the nature of this involvement is unclear. Does it go as far as CCB initiatives such as the Global Forum for Cyber Expertise, which have full private sector members?[58] The nature and extent of private sector involvement in CCS mechanisms will be decisive in shaping their priorities, capacities, and abilities to scale. This paper recommends that actors looking to establish or improve a CCS mechanism put significant effort into considering private sector involvement.

A comprehensive approach to international cyber support. CCS mechanisms are largely being developed by actors who are already engaged in some kind of international cyber support activities. For some actors these mechanisms are entirely novel, for others they are based on previously ad hoc processes or are derived from other areas of policy, such as humanitarian support or military assistance. While this report welcomes greater attention to CCS-like functions, it strongly recommends ensuring that a focus on CCS, and particularly emergency provision, does not crowd out other international cyber support. As detailed above, CCS should not come at the expense of CCB – long-term, sustainable interventions to build the recipient's internal capacities. Committing resources to responsive capability provision seems to address more urgent needs, but it may not be the most efficient way to address foundational challenges. Ultimately, neither CCB nor CCS can cover all facets of international cyber support. Actors should instead leverage diverse tools across a spectrum of international cyber support activities which are prioritised and deployed based on their strategic objectives.

57 Beecroft, 'Evaluating the International Support to Ukrainian Cyber Defense'.
58 'Members & Partners', GFCE, accessed 10 January 2024, https://thegfce.org/member-and-partner/.

5. CONCLUSION

Large-scale, national cyber incidents and events have been a fixture of recent years. International responses to these have been significant and, in most cases, have been conducted on an ad hoc basis. The creation of new CCS mechanisms begins to provide more clarity on how, where, and with whom actors intend to provide support.

This paper has argued that multiple national and international actors have begun creating and scaling CCS mechanisms and that many of these emerging initiatives show promise. It has analysed existing and proposed mechanisms to identify factors that shape the provision of CCS and has advocated that these and other identified lessons be considered by actors operationalizing CCS. Furthermore, it has argued that outlining a clear strategic objective, considering multi-stakeholder collaboration, and creating a comprehensive approach to international cyber support are key to effective CCS.

To put these arguments forward, this paper has proposed CCS as a policy area and has drawn a distinction between it and CCB within broader international cyber support. While this paper acknowledges that such a reconceptualization requires further discussion, it maintains that distinct policy instruments are useful to meet separate outcomes and impact objectives.

Section 2 of this paper outlined case studies of national cyber incidents in Ukraine and Costa Rica and the ad hoc response from actors operationalizing CCS. Section 3 then analysed emerging, existing, and proposed CCS mechanisms to identify points which affect their organization, remit, thresholds, activities, and private sector involvement. Lastly, Section 4 outlined considerations for operationalizing CCS across alignment, enabling environments, monitoring, and measurement; it also proposed urgent points for actors to consider.

Further research on this topic should examine how the strategic value-case of CCS mechanisms affects their implementation and the factors that determine the participation of multiple stakeholders. As part of efforts to reevaluate international cyber support, policy-focused research creating a typology of activities would be invaluable. Furthermore, research on CCS funding and procurement mechanisms will help ensure the efficiency of emerging mechanisms. Finally, comparative in-depth analysis should be conducted on CCS in various large-scale national cyber incidents to identify tactical and operational best practices.

ACKNOWLEDGEMENTS

I am grateful to the reviewers of this paper for their patience and the significant time and effort they have expended in providing comments and suggestions.

I am also appreciative of insights received from friends and colleagues, including within the RUSI cyber team – specifically, the shrewd recommendations of Pia Hüsch, Hugh Oberlander and Conrad Prince.