CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

NATO Cyberspace Exercises: Moving Ahead

CyCon 2022 Workshop Summary

Amy Ertan, Veronika Datzer, Aurimas Kuprys, Lisa Schauss

NATO CCDCOE

Released December 2022

This summary report reflects the output of the CyCon 2022 workshop on NATO cyber exercises. It draws on endeavours over the previous two years to bring together relevant experts from national militaries, NATO, academia and industry to discuss contemporary challenges and opportunities for effective exercising across the cyber domain.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the Centre is a diverse group of international experts from military, government, academia and industry, currently representing 38 sponsoring and contributing members.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

Acknowledgements

This workshop could not have taken place without support from the international expert community and from all those who contributed to discussion, and logistics, on the day. We would like to thank the staff at the NATO CCDCOE for supporting this workshop for the second year running, with particular thanks to the CyCon 2022 organising committee and support staff. We are grateful to our expert speakers on the day: Dan Black (NATO Headquarters), James Reynolds (United Kingdom Delegation to NATO), Sven Rieche (NATO Allied Command Transformation Headquarter), Sergio Ricardo Caldeira de Carvalho (Cyber Defence Centre, Portuguese Armed Forces), Lauri Almann (CybExer Technologies) and Miriam Nasser (Microsoft). We offer our thanks to Veronika Datzer, Peadar Callaghan, Olena Roraff, James Barr, and Sophia Escobar, who acted as scribes through the session and thus informed the edited summary contained in this report.

Steering Committee:

Amy Ertan, Aurimas Kuprys, Pilleriin Lillemets, Gry-Mona Nordli, Lisa Schauss

Table of Contents

1. Introduction and context

How do we effectively "train as we fight" in cyberspace? How can NATO best adapt to changes in the cyber threat landscape, or themes including hybrid warfare and disinformation which blur the distinctions between kinetic and digital warfare? How can Allies overcome the challenges of information-sharing and duplication to ensure swift response to adversarial attacks - and how can exercising facilitate such shifts? These questions represent active areas of discussion across the NATO Enterprise, as the Organisation continues to build out the effective design, execution, and strategic development of cyber and joint military exercises.

At the 2022 International Cyber Conflict Conference (CyCon) the workshop "NATO Cyberspace Exercises: Moving Ahead" took place. For the second year, this NATO exercise-focused workshop gathered experts to address and discuss these concerns. Held in person, the workshop welcomed approximately 65 attendees including a range of invited experts and relevant stakeholders, as well as open sign-ups from conference attendees who were interested in cyber exercising themes. This workshop drew upon the valuable input and recommendations captured from the 2021 workshop, further opening the conversation on NATO exercises to the broader cyber community. Following plenary presentations, attendees were divided into six-eight person syndicates to discuss relevant challenges and opportunities. The workshop ran in accordance with Chatham House convention and as such syndicate comments are not attributed to any attendees by name.

This report summarises the main discussion points from this workshop.

Previous reports in this series:

CyCon (2021) workshop summary report:
"Cyber Exercises: A Vision for NATO"

Interim paper (2021):
"Trust in Cyber Exercises: A Vision for NATO"

2. Scene setting and keynote:

Dan Black, Principal Analyst, Cyber Threat Analysis Branch, Joint Intelligence & Security Division, NATO

Reflecting on the war in Ukraine, Dan highlighted the new reality of cyberspace as NATO's most contested domain and the primary area for competition between states. Russia's unprecedented use of cyber operations in Ukraine highlights several major implications for NATO exercising efforts:

- Cyber exercises represent an opportunity to develop and test national responses in a safe environment.
- NATO has the capability to facilitate information-sharing and bring together communities, strengthening collective security through stress-testing exercises and coordinating large-scale operations.
- There will be "first-move" advantages for early adopters of emerging technologies within multi-domain warfighting.
- Cyber themes pose strategic challenges. The activity in Ukraine highlights how cyber operations may provide the basis on which to trigger NATO's Article 5 on collective defence, which would be decided on a case-by-case basis by the North Atlantic Council.

Dan emphasised that while there is an unpredictable security environment ahead, NATO recognises that cyberspace will continue to be at the core of strategic competition and conflict. NATO continues with commitments to improve its defences and continues to encourage international collaboration to enable greater Allied resilience.

3. Main findings

Discussions through the workshop are categorised into four themes: trust and information sharing; NATO and national cyber exercises; designing scenarios to meet Training Objectives; and "What next?".

3.1 Trust and Information Sharing

Participants broadly agreed that cyber exercises require trust. Joint cyber threats, common interests, and mutual benefits were identified as drivers to enhancing trust amongst NATO Allies. Exercises were seen as one way to steadily develop trust and information-sharing practices between Nations, with the understanding that information-sharing must be a two-way process and states cannot expect to receive information without offering information of their own. Participants agreed on the principle of incremental, steady increases in information-sharing to build "trust through credibility", as the provision of reliable information leads to perceived legitimacy.

The conversation focused on the following topics:

- **The role of trust in collaboration across nations/ security organisations**

  The discussion on what kind of information and personnel should be involved led to particularly intense debate:

  - Participants argued that leadership-level staff should be the first involved in exercises to create momentum for operational teams, as high-level information is more easily shared.
  - Other participants noted that trust should be built "bottom-up" and that the sharing of technical and operational information in exercises would increase the learning possibilities.
  - Participants distinguished "learning" and "competition" based exercises – if there is a score for an exercise, there may be less willingness to make mistakes and show vulnerabilities.

- **Challenges to trust-building in cyber exercises**
  - Emerging costs were identified as challenges to trust-building in cyber exercises. To mitigate the financial burden, participants generally recommended governments co-partner with the private sector. Participants highlighted the need for trusted government partners to be involved in exercises.
    - Participants agreed that some private sector organisations now have increased involvement in this space due to their provision of centralised platforms. However, some participants raised suspicions of private actors who are not accountable in the same way as elected governments.
  - Differences in regulations across the international spheres and the involvement of different sectors were identified as challenges to information-sharing in exercise scenarios.
  - Participants debated the tension between data mining and protection of sources or of industry data provided by entities for exercises. Anonymising incoming data can be particularly important to avoid vulnerabilities being used against a person or entity.

        - It was discussed whether MISP[1] Threat Sharing should be made more anonymous.
    - Participants made a point of clear differentiation of "information sharing" vs "intelligence sharing". While the former needs to be open and transparent, the latter does not.
    - Another point of discussion was the classification of information. Participants agreed that oftentimes information gets much higher classification than necessary, which prevents it from being used or acted upon.

- **Opportunities to improve trust and information-sharing amongst Allies**
    - Participants highlighted the importance of:
        - Adequate planning of exercises and measuring the effectiveness of cyber exercises across borders;
        - Clear communication of the expectations of cyber exercises as a key to building trust in cyber exercises and their relevance;
        - Gamification, time, and personal interaction as potential trust-enhancing factors.
        - Transparency: Ukraine's approach to information-sharing was considered particularly transparent and a potential role model for future information-sharing beyond the Alliance. Participants also felt classification needs to follow more transparent and should be aligned across NATO members.
    - Discussions had several suggestions for trust-building measures including:
        - An interoffice taskforce as a method of building international cooperation across several silos and;
        - More small-scale exercises with clear tangible goals and clear expectation management (avoiding any blurring between offensive and defensive-focused cyber exercises);
        - A common standard for information sharing. If the situation allows, participants encouraged the establishment of a default system instead of a need-to-know-system, to encourage further dissemination.

3.2 NATO & National cyber exercises

The second discussion session focused on ongoing collective defence efforts and cyber exercises. In discussing this theme, the conversation focused **not** on the well-understood principle of collective defence as set out in NATO's founding treaty.[2] In this workshop, the phrase "collective defence" referred to the distinct concept of how NATO can best ensure the continued resilience of Allies on an ongoing basis, for example through cooperative capability building-measures and trust-building, with particular focus on the following sub-themes:

- Allied cooperation in cyberspace
    - Participants debated the nature of daily "collective defence"-related activities at length.

[11] Malware Information Sharing Platform: an open source threat intelligence platform through which information including indicators of compromise, vulnerability information and threat intelligence can be shared within a trusted community. See https://www.misp.software/index.html.

[2] Article 5 of the Washington Treaty enshrines the principle of collective defence, which means that an attack against one Ally is considered an attack against all Allies. This enduring commitment lies at the very heart of NATO's solidarity and Allied security and solidarity. For more information on the principle of collective defence and Article 5 see https://www.nato.int/cps/en/natohq/topics_110496.htm.

  - Information-sharing, while difficult, is considered the foundation of collective training and participants highlighted opportunities for enhancement.
  - Participants mentioned that collective defence requires or builds on extremely close ties amongst partners including a high willingness to share information and vulnerabilities. This is currently not the norm, especially in the cyberspace domain. This discussion addressed the common interests of Allies in terms of cyber defence and resilience across the Alliance.
  - Participants referred to NATO's Article 3, which states that every Nation is responsible for the defence of their own networks. There was debate how this aspect plays into collective defence.
- How collective exercising can benefit Nations
  - There was extensive discussion on how collective exercising can benefit NATO and deliver advantages for Nations. While syndicate participants agreed on the importance of collective exercises to further knowledge, enhance skills, and improve capabilities across NATO Nations, the discussion about how exercises might be adapted to better enable cooperation across the Alliance was significantly more fractured.
  - This was in part due to different understandings of collective defence as participants disagreed on how far complete sharing of information was fully achievable, with some Participants highlighting that Nations, even if they all share the basic need for exercises, are at different points on the learning curve. It proved difficult for participants to find a coherent basis on furthering NATO's exercises to ensure strengthened cooperation between Allies. When discussing NATO's contribution towards national capability development efforts, participants highlighted that the diversity between nations and their differences regarding capabilities, possibilities, objectives, legislations and resources are very difficult to overcome.
  - Some participants suggested the creation and use of "plug and play" exercises, where NATO would build flexible exercises that would allow Nations to tailor them to their own needs by choosing relevant topics or modules and bring Nations up to a similar standard. Participants suggested this may provide a good foundation for collective training, which ultimately contributes to a stronger cyber defence posture across the Alliance.

- Difficulties in sharing national Lessons Learned (LL)
  - Whilst participants agreed on the importance of trust and information sharing, discussions repeatedly acknowledged that there are many barriers to effective sharing post-exercise. This makes it harder to implement a beneficial Lessons Learned process.
  - Nations currently do not want to or are not able to share LL as it can reveal weaknesses and vulnerabilities in their systems, and/or potentially disclose confidential information.
  - Participants also raised the issue of culture as an important factor. Some militaries would require cultural change to improve the LL process. Within NATO such a cultural adaptation would need to be implemented across many Nations.
  - Participants also agreed that information sharing, although very difficult, is the basis of collective training to improve capabilities, integrate Nations, further common interest and ultimately build a basis for collective defence.
  - Participants also discussed the need of a simple and effective sharing platform, which might also offer the chance to automate the LL process, though this still has a long way to go.
  - Participants also suggested that holistic discussions on exercise design at NATO should take place more frequently. These discussion forums may also benefit from greater engagement from a diverse range of stakeholders beyond current exercise coordinators. These discussions could take place as follow-on events after exercises to best leverage Lessons Identified.

- Participants suggested greater effort be taken to identify and engage key stakeholders that can be invited to discuss challenges and possibilities across silos.

3.3. Designing scenarios to meet Training Objectives

During this discussion, participants identified multiple interconnected challenges related with building cyber exercises including but not limited to: duration of the planning – preparation – execution cycle; the scope preparation effort; identification of the Training Audiences/ selection of the Training Objectives; stakeholders buy-in; and the content of the scenarios. These themes are discussed in turn:

- The planning cycle for NATO Exercises
  - The typical planning – preparation - execution cycle of the NATO exercise normally lasts up to one year or even longer, with multiple planning events and many work hours to prepare the exercise plan and other supporting documentation. The length of the cycle and limited robustness of the planning process does not facilitate integration of recent events and technological developments into the scenario, leaving the exercise focused on the past instead preparing Training Audiences to deal with emerging threats and future technologies.

- A need for better stakeholder engagement with Training Objectives
  - Large scale exercises usually also have many different Training Audiences with varying levels of competence and experience. Exercise planners, aiming to accommodate their diverse training needs, are forced to seek compromises that regularly lead to suboptimal solutions.
  - At the same time, while building the exercise design, exercise planners often fail to consider if all Training Audiences should be trained to the same extent (e.g., the technical level activities and procedures do not change so dynamically compared with developments at operational or strategic level seen in recent years).

- A need for appropriate realism in exercise design:
  - Participants agreed that well-designed storylines are a critical factor in implementation of successful cyber exercise. These storylines enable the delivery of a clear set of learning goals and provide a clear direction and scope for the exercise.
  - Participants also highlighted the vital need for and importance of a common basis for transparency, information sharing and validation in order to develop collective exercising and work towards a common goal and collective defence.

Participants provisionally agreed on several suggestions to address these limitations, including that:

- Exercise planners should reduce the ambition towards the scope of the exercises and focus on quality transitioning towards smaller scale modular and reusable exercises: scenarios which can be easily updated and custom tailored in accordance with needs of a particular Training Audience, while at the same time providing the benefit of comparably low costs.
  - “Small scale exercise” should not be understood as exercises with limited Training Audiences. Such exercises should, participants argued, instead bringing cross-functional or inter-disciplinary Training Audiences together.

- Exercise planners should engage in active dialog with leadership, Training Audiences and other stakeholders getting their input and building consensus on the Training Objectives. This would later ensure wider acceptance and "buy-in" of all involved parties.
    - It was generally agreed that the Training Objectives should be limited in scope. They should be as simple as possible to avoid unnecessary complexity, as they can be achieved only if they are understood by everyone involved.
    - When discussing which themes should be considered while building Training Objectives, participants generally proposed the following general categories:
        - Incident handling and response (to test procedures and capabilities);
        - Reporting and information exchange both along vertical channels of communication (to enhance situational awareness and decision making) and horizontally (to ensure better coordination between entities involved);
        - Conducting full spectrum cyberspace operations (to build understanding of policies and operational concepts, and to improve integration of capabilities and coordination with other domains).

- Exercise planners should find the balance and avoid creating over-simplified "theoretical" storylines which may discourage participants or fail to bring necessary learning experience, while at the same time refrain from building over-complex and out of scope storylines that may distract participants from achieving the Training Objectives.

3.4 Moving forwards: What's next?

The final presentation and syndicate session focused on the question: "What's next?", aiming at challenging the audience to think about how to overcome future information sharing challenges in cyberspace exercises. The brief highlighted how public-private cooperation can facilitate interoperability, though highlighted the challenges of insufficient trust, the lack of widely accepted open standards by NATO communities, and the lack of common vocabulary as barriers to effective information exchange.

Major themes discussed through the presentation and syndicate breakouts include:

- Interoperability
    - Participants noted that data is captured and used in silos at NATO, and highlighted that a common platform could facilitate more effective data management practices. Participants also suggested the that need for more work to share data outside the network of NATO members to ensure NATO partners have access to relevant information, and work to clearly classify data appropriately across private and sovereign silos.
        - NATO is working on these issues to adopt common rules and protocols such as federated mission networking (FMN).
    - Open standards were proposed as a recommended path forwards as participants highlighted the importance of a common language in information-sharing, as well as legal mechanisms to share appropriately. As there are already open standards available, some participants recommended NATO should work to formally agree and incorporate common standards as established architecture. Nations do not agree with a standard, they should be involved in the committee around changing and creating standards.
    - Participants noted that exercises should recognise that not every Nation has a "Cyber Command". Where Nations have a Cyber Command, responsibilities for cyber defence, roles and responsibilities are often divided between different administrative, civilian and military entities and this shapes how they interact in NATO exercises. Participants also noted that in an ideal world, nations should have a coordinated and connected national approach to cyber defence, which enables engagement with realistic holistic cyber exercises.

- Operationalising the Lessons Learned from cyber exercises.
    - Participants viewed Lessons Learned information as a productive area to improve the regular exchange of information for the benefit of the Alliance. Recognising that Lessons Learned outputs continue to be under-utilised, there is value in sharing and operationalising Lessons Learned before the onset of the next exercise. The vast amount of data output from exercises raises the possibility of utilising technologies to analyse that data and forming an input into Lessons Learned, though this requires a trust in such technologies to work reliably.
    - Participants agreed there should be more emphasis on implementing Lessons Learned and improving Lessons Learned processes. Suggestions included the greater use of mechanisms to track Lessons Learned, and to assign accountability to ensure that the Lessons Learned as a result of NATO exercises are incorporated into national processes.

There should be increased efforts to incorporate emerging Lessons Learned from Ukraine into future exercises.

4. Conclusion

Much of the discussion in the workshop focused on how to incorporate real world events, including aspects of the ongoing war in Ukraine, into exercises to best prepare defenders. The final discussion made several proposals that included recommendations for NATO to agree on standards for information sharing, for the establishment of one platform to share cyber information between Members (building on successes with mechanisms such as MISP), and to clarify data classification mechanisms to classify appropriately but minimise tendencies to overclassify information. Despite the challenges in information sharing and building effective exercises based on trust, there is a clear wish within the community to do more and do better together.

Several themes resurfaced throughout the syndicate sessions, including the level of ambition, sharing lessons, learning to be transparent and trusting in sharing information. There is an underlying sense of urgency and need to work together to the face of common adversaries and challenges, from Russia's war in Ukraine to the unknowns of emerging and disruptive technologies.

As NATO considers the effective design and conduct of cyber exercises, several paths forward draw on these themes. From the creation of appropriate Training Objectives to efforts to become comfortable with new technologies and data management approaches, it is clear that NATO will need to continue to adapt to the changing security landscape. Now more than ever, it is essential that cyber exercises are utilised to develop trust across the Alliance, and between Allies and trusted partners. As a range of participants noted, exercises will continue to play a fundamental role in cyber defence and resilience.