CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Cyber Exercises: A Vision for NATO

CyCon 2021 Workshop Summary Report

Amy Ertan, Lt. Col. Aurimas Kuprys, Pilleriin Lillemets, and Lt. Col. Gry-Mona Nordli

Special thanks to Commander Robert Buckles

NATO CCDCOE

Released 19th August 2021

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 35 sponsoring and contributing members.

www.ccdcoe.org

Disclaimer

Table of Contents

1. Introduction and Context

How do we best incorporate the cyber domain into joint exercises, highlighting security implications for entrenched dependencies on technology and internet-connected systems? What is NATO's vision for effective cyber exercises, and how does this correspond with Members' national exercising goals? How do NATO, and other multinational exercises, approach the challenges of limited trust or unclear learning objectives, and work to ensure exercises complement each other? Who provides input into multinational exercises, and who should?

The Cyber Exercises workshop at the international Cyber Conflict Conference (CyCon) 2021 was designed in response to these broad questions and concerns. As an organisation, various agencies at NATO run a number of cyber-specific exercises, as well as broader exercise and simulation activities. In order to identify gaps, overlaps, challenges and opportunities for NATO-facilitated cyber exercises, workshop committee members agreed a workshop must consider the bigger picture of cyber exercises. This involved creating a space which invites NATO colleagues who are integral to the exercise design, development and delivery process, NATO policy-creators, as well as external colleagues who could highlight national, industry, and academic best practices.

This document provides an overview of the workshop including key themes raised by invited speakers and through syndicate 'break-out' rooms over the course of the workshop. The document also includes a section on 'recommendations' drawn throughout the session.

The workshop was held virtually on MS Teams with 50 attendees drawn from the US, Australia and across Europe. All those who attended were invited due to their professional experience relating to cyber exercises. In addition to relevant speakers, attendees represented a range of NATO and CCDCOE member nations and also included colleagues contributing to a range of NATO exercises. Following plenary presentations attendees were divided into 4-6 person syndicates to discuss relevant challenges and opportunities. Topics that were covered in these discussions varied from syndicate to syndicate and have been compiled below. The workshop ran in accordance with Chatham House convention and as such no attendee names or attributed quotes are included in this summary, with the exception of the committee and opening keynote speaker General Patrick Sanders.

2. Main Themes

The workshop highlighted a number of relevant issues and opportunities when considering NATO's 'Vision for Cyber Exercises', with discussion often drawing on the following main themes:

- **Trust is essential.** NATO and national militaries must determine how to share training information without sharing vulnerabilities. This is also a challenge for integrating outside groups into training as militaries must develop the required trust levels with the assurance that sensitive information will be protected within the trusted network of exercise members and partners.
- **People are central to cybersecurity.** Security depends on *people* and *culture*. Militaries need to understand the training audience to make training effective. Cyber is also a team sport, and colleagues across NATO and militaries should be engaged and informed on the importance of recognising wider audience needs and perspectives on cyber security, in two-way information exchange.
- **Exercising 'in the right way'.** NATO must increase the scope of involvement in cybersecurity but *in the right way.* Training objectives should bear in mind the challenges around integrating cyber into joint training, and the support that should be provided to training audiences across the Alliance. Exercises should be realistic and mirror the real world as far as this allows the goals of the exercise (for example collaboration) to be realised.
- **Complementing, not duplicating.** NATO objectives will differ from those of its individual members. However, NATO provides a unique platform to host large-scale exercises to test military cyber capabilities and try out new doctrines. There are opportunities to complement national training exercises as well as inform and assist members in capability building when it comes to cyber education and training.
- **Coordination between exercises.** Exercises require clear scope and should extend beyond the 'cyber' bubble to reach out to broader military structures. Senior leadership should be involved, with NATO and militaries benefiting from a top-down approach to cyber exercises.

The workshop committee continues to work on these topics. A more detailed report is planned for future dissemination alongside initiatives to inform cyber exercise design and deployment across NATO.

3. Keynote: General Patrick Sanders, Commander United Kingdom Strategic Command

General Patrick Sanders opened the workshop, sharing both a vision for the UK's approach in preparing for cyber threats as well as how NATO has and could further position itself in promoting a shared deterrence strategy. Reflecting on an increasingly complex and competitive threat landscape, and the potential for disinformation and malicious cyber activity to undermine societies, the General stressed it is critical for NATO to foster responsible action through:

- Stressing the values and importance of a free, stable, and secure Internet.
- Norms-building through which International Law is respected in cyberspace, facilitating discussion on how these rules and norms will be applied by states.
- Reinforcing the role of NATO as a platform for collective action and allied nations on cyber matters.

The General acknowledged a series of considerations for NATO, expressing the view that NATO needs to be more prepared to discuss what can be considered malicious cyber activities. The UK recognises the need for cross-domain deterrence and has focused on strengthening multi-domain integration. There is a need to ensure how industry is best incorporated into cyber defence activities, recognising NATO member reliance on commercial networks and supply chain security challenges. There is also a need to test capabilities in cyber exercises in a way that considers the political sphere and strategic decision-making, and considering how to provide relevant information to decision-makers in a timely manner.

Discussing the creation of a deterrence strategy, General Sanders highlighted Cyber Coalition as a cornerstone NATO exercise and platform for experimentation and validation of concepts, which is complemented by technical exercises such as CCDCOE's Locked Shields. Looking at what deterrence should do, the General stressed the need to continually develop and test defences through experimentation, exercises and wargames. NATO and members should expand scenario-based discussions, drawing on the technical, military, strategic and political spheres.

4. NATO Perspectives

The NATO brief identified a number of challenges in the way cyber exercises are currently planned and conducted:

- **Difficulties integrating cyber into joint functions and battle rhythms**. In order to succeed with this, NATO must have a clear vision of what the Alliance is trying to achieve when talking about cyberspace as a domain of operations. In addition, there needs to be an increased willingness to give cyber a bigger role in Joint exercises.

- **The difficulty of translating technical data about cyber-attacks into meaningful information for decision-makers represents another challenge when integrating cyber into broader exercises**. This effort requires a comprehensive understanding of roles and responsibilities and an understanding that there are different requirements at different levels. At the strategic level, the focus is on policy, while at the operational level, the focus is on C2, situational awareness, and crisis management. At the tactical level, exercises are more about sharing tactics, playbooks. More work is needed to understand these roles/responsibilities at the tactical level.

- **NATO needs multidisciplinary specialists with a broader understanding of the characteristics of a domain built on technology.** To integrate cyber into Joint exercises and do it in a way that the training requirements on all levels are met, NATO needs to be training teams of experts, not just expert teams made up of colleagues with computer science and/or technical backgrounds. We need to develop collaboration and communication skills. The team needs to combine multiple roles, and they need to collaborate effectively.

- **Trained individuals who are trained are then rotated back out to national forces**, which underscores the importance of aligning NATO and national-level training.

All of these challenges have a common link back to gaps in individual training. How do we measure success in training individuals and collectives? To have successful exercises, NATO must ensure that our training objectives are correct. One way to better integrate NATO and national training would be through more extensive use of Cyber Ranges. A NATO cyber range is not sufficient by itself and needs to be supplemented with national cyber ranges, with opportunities to link national and NATO functions/exercises. For example, data from national cyber ranges could be used to identify training gaps at national levels to be addressed through NATO.

5. National Perspectives

As different organisations and nations have their own ways of approaching cyber exercises the workshop invited representatives to present different perspectives during the workshop. Speakers from the UK and the Netherlands both gave presentations on their national approaches to cyber exercises and provided some insight into how NATO and nations can benefit from their experiences, giving examples of some training arenas they attend and highlighted some key takeaways to consider when planning and conducting national exercises or attending NATO exercises with a national team.

The tabletop format was highlighted as the best exercise method for training policy and decision-makers. This approach requires technical provision and is relatively less costly, but requires well thought through preparations. This approach pushes the exercises through a very compressed timeline.

Major themes discussed through the presentations and syndicate breakouts include:

- **Multi-Domain Integration**
    - Defensive Cyber Operations were highlighted as a part of multi-domain integration, with ideal – inclusion of cyber content in major incidents on three-star or two-star headquarter exercises. There are, however, issues around domains being excluded during exercise if the focus is purely on cyber for example. One potential pitfall the presenter warned about was the issue of attribution. Under normal circumstances, this is a time-consuming process and exercising this in short exercises may create a false impression of the required time to conduct attribution. The issue of offensive cyberspace operations may also cause further complications as this is dealt with at a higher level compared to other domains.
    - There is a lack of understanding of the operational impact of cyber effects. Senior leaders don't necessarily understand what vulnerabilities are, or the implications of a cyber effect.
    - NATO is fulfilling its core tasks through operations and must therefore incorporate cyber considerations, making cyber a natural part of any exercise and not just developing separate exercises for cyber. To achieve better integration of cyber into operations the cyber domain should not be treated as more special than it is.
- **Trust and sharing Lessons Identified/ Lessons Learned**
    - Exercising as NATO helps creates shared behaviours across countries. However, nations are reluctant to share tactics and procedures as this may give away knowledge of their own vulnerabilities, a symptom of the wider issue of trust issue within the NATO alliance. Sharing lessons learned/identified is sharing your weaknesses, and few want to share that information.
    - NATO does not generally share lessons learned between different training audiences. While NATO does have a strong lessons learned/identified process, nations usually don't want to share lessons identified about their problems.
    - NATO has the potential to facilitate sharing of 'best practices' – something that does not involve revealing secrets/weaknesses. In the NATO Lessons Learned Portal, there is a

Community of Interest where sharing lessons within the cyber community is possible. This feature is unfortunately relatively unknown and therefore hardly used.

- Some attendees viewed offensive and defensive cyberspace operations as a sovereign capability (drawing parallels to nuclear weapons). When a nation trains their crew or experts on systems, they don't want to share that knowledge with other parties. Crew/unit would do specific evaluations so they know the vulnerability of crew/ship, and this would be considered highly sensitive information to be protected. So on exercises, you see the skills of other units, but will also see the weaknesses, so it can be compared to nuclear in that sense.
- It is challenging to share information at different classification levels across NATO, and attendees presented the view that there is significant over-classification that is not only hampering the sharing between nations but also between organisations within the same nation.
- This is not restricted to classified information; there are aspects that must be tested nationally to measure how a country reacts to certain cyber scenarios that are not classified. When NATO works at a national level it helps develop a sense of relevant sectors and actors within the national and international cyber landscape. Rehearsing the impact of legislation is also an integral component of exercises, and can be integral to learn from others at an international level.

- **Effective Exercise Design**
  - The goal is to train as you fight, and there are several ways of simulating real-life environments to conduct exercises in. However, it is not often we are able to fully replicate operational networks; effective exercise design will consider the training audiences' real-world practices to design an appropriate and realistic scenario. Increased realism can also be achieved by including industry and the private sector. Participants' failure in an exercise should not necessarily be viewed as something entirely negative, it can be seen as a part of the process as long as no harm is done other than causing some embarrassment. Well-designed exercises provide the training audience with a safe environment to experiment where one can fail without major consequences.
  - Cyber threat-related intelligence is key to driving threat scenarios in a given exercise. A staff officer from any given country that comes to NATO may be an intelligence analyst with no cyber expertise or a cyber analyst but without much intel experience, Intelligence Operators are very scarce beasts. Attendees considered it more straightforward to take those with cyber security expertise and teach them intel practices, than the other way around.
- **Recognising National vs NATO objectives**
  - National exercises will have different priorities than NATO exercises, but there is a lot of potential for nations to use training arenas provided by NATO for national training. Training objectives are often the same between NATO exercises and national exercises and it is also easier to efficiently combine exercises when the exercises are built on the same scenario.

- Exercising offensive cyberspace operations is usually kept at a national level, but needs to be integrated as a NATO capability, and should be trained as such too. It needs to create links to those nations that have offered up these capabilities.
- In terms of collaboration on national exercise planning, there should be a NATO initiative to invite member states to gather exercise developers in a working group harmonising both national and NATO exercise planning and training. NATO is currently developing a training solution to provide training for exercise planners contributing to both cyber exercises and joint exercises where cyber is being trained.
- In terms of what NATO can learn from national exercises, there needs to be creativity within NATO – across targets, training requirements. NATO cares about critical infrastructure when it affects the military operations and effectiveness. But from a national level, critical infrastructure is important for a wider range of reasons. Like the EU, NATO should build upon the national approaches such as including public and private sector challenges such as critical infrastructure.

6. Perspectives from Industry and Academia

With innovation in various forms, additional dimensions were added to warfare, introducing naval warfare, adding air and then space. Notwithstanding multi-dimensional complexity, warfare remained quite homogenous and deterministic, with warfighting based on formations, dispositions, and series of manoeuvres. The inclusion of cyberspace as the 5th domain of warfare introduced an additional degree of unpredictability. In order to fight and prevail in the contemporary battlefield, we have to train in scenarios that encompass a certain level of anarchy and chaos, mirroring the chaos produced by both friendly actors and adversaries in the wild.

NATO and national militaries tend to exercise cyber in isolation, in relatively sterile environments where only our own and enemy systems operate. This approach creates artificiality into an exercise: leaving the majority of cyber actors outside of exercises' scope, while in real life, a crisis would involve the rapid engagement of a range of actors including civilian entities, governmental agencies and industry. While NATO has predicted that the next conflict will be hybrid, however, the participants' view was that this is not reflected in NATO cyber exercises. The civilian sector and the rest of society may help create depth of the defence and could be a source of reserves for the military as well, and by getting out of the "bubble" and expanding engagement with the private sector NATO could benefit in many aspects.

Moreover, NATO and military organizations should learn from civilian entities as they are already constantly engaged in cyberspace operations, even in peacetime. Many have employed ex-military or reservists, who, with their unique knowledge and experience gained operating as a part of both military and civilian organizations, could be extremely valuable in strengthening cyber capabilities.

Presenters at the conference highlighted that while military organizations have been benefiting from cooperation with industry and academia for a long time, traditional military secrecy and mistrust towards outsiders prevent military organizations from getting the full value of learning from partners. In order to gain full value from engagement with industry and academia, military organizations should get rid of traditional thinking that sharing information may expose our vulnerabilities to adversaries, and embrace a new paradigm that training together and sharing information will allow for all involved to become stronger.

Industry and academia are often discouraged from participation in exercises with military organizations due to the fact that much of the military content will be classified, preventing them from being able to refer to specifics learned during exercises. To address that issue the exercises should be designed in a manner that would facilitate the participation of diverse audiences and would ensure fulfilment of classification requirements.

The level of cooperation of governmental and private organizations varies from nation to nation. Industry willingness to engage differs depending on whether the counterpart is civilian, a governmental organization, or military. Thus, it may be challenging to confirm a model facilitating external (industry and academia) involvement in cyber exercises that would work across NATO, however, the application of compartmentalized formats to exercises may help facilitate engagement in less sensitive contexts.

And last but not least, attendees reflected that cyber exercises used to aim to surprise audiences, as training scenarios were designed to prepare us for a possible future. As time passed, those scenarios started to resemble the current real-life context more and more, while, at the same time, our performance in exercises became better and better. Meanwhile, replication of the real world context, with chaos and attacks occurring from unexpected angles, could be ensured by introducing an 'Opposing Force' that would act in accordance with a given mission but would be free to choose the ways or direction from which to attack.

7. Recommendations

As a result of the workshop syndicates a significant number of opportunities for improvement, and correlated recommendations, were proposed by attendees. Recommendations are categorised as follows, highlighting that colleagues who are responsible for developing and delivering cyber (or joint cyber) exercises should:

- **Ensure that exercises should be clearly defined.** This includes identifying the purpose of the exercise: are participants engaging with the exercise aiming to compete, learn, or rehearse a known set of actions? Alternatively, should the exercise be designed to test and validate procedures?
- **Increase focus on the development of Training Objectives** and where they overlap between NATO and national exercises. Using the same scenario for NATO and national exercises might reduce the number of exercises needed to achieve the Training Objectives.
- **Know the training audience and the motivation for the exercise.** The needs of the training audience should determine the process and shape of the exercise.
- **Identify the necessary interactions in the process being exercised.** Getting a clear view of how interactions will take place through the exercise helps identify the type of role-playing required to help the training audience best work through the exercise.
- **Create a pool of subject matter experts.**
    - Cyber military reserves could help fill this role if they are trained according to established procedures
    - This may involve embedding industry partners as players in the exercise.
    - The training audience can benefit from using and incorporating them into the exercise.
- **Exercise future potential scenarios.** We should not forget that the aim of exercises is not to help us be good at exercising but to be effective in modern conflict and there is, therefore, a need to create exercise scenarios based on assumptions about how the future will be different from contemporary situations, far outside of our comfort zone. Creating realistic exercises scenarios reflecting comprehensive models of the future will require the involvement of a wider spectrum of entities across NATO. Engagement of various NATO entities together with industry and academia partners in exercise scenario development would enable modelling of future and creation of comprehensive and realistic training scenarios.
- **Embrace different classification requirements of all involved parties**. The challenge of diverse security and classification requirements of different entities that prevent the inclusion of external partners into the exercise could be mitigated by creating a compartmentalized training environment with separate classified and unclassified segments that would allow the involvement of a wider spectrum of participants.
- **Recognise training fatigue as a risk** and plan for sustainable participant engagement with cyber exercises, There needs to be time in-between the exercises not only for the training audience to do their regular job, but also to implement the lessons learned from the exercises. Including reservists in exercises will not only provide these individuals with important training but also help reduce exercise fatigue.
- **Increase use of red teaming for joint level exercises.** NATO needs to increase cyber range usage, with red teams as well as the use of red teams in live networks as well as the inclusion of broader adversarial behaviour (including in strategic and operational terms). The inclusion of red team behaviour as an opposing force will better replicate realistic adversary behaviour.
- **Cyber effects need to be exercised and integrated more into the exercises,** and there needs to be an increased willingness to give cyber a bigger role in Joint exercises. Often we see that we are not allowed to play the cyber scenario to its full extent as that would shut down the whole exercise. Cyber should be considered throughout the operational domain. If we are to succeed in implementing the Cyberspace domain, we need to make cyber a natural part of any exercise and not just develop separate exercises for cyber.

- **NATO and national training should be aligned to close the gaps in the individual training.** The Cyberspace Operations Annual Discipline Conference (ADC) provides a good opportunity for nations to provide their contributions to the Training Needs Analysis process. The ADC can support the nations both by providing a primary forum to review and update education and training requirements, and by helping nations align their requirements and training needs with those identified by NATO.

8. Closing Remarks

This workshop highlighted that there are many future paths forward for cyber exercises, within and beyond NATO. A Vision for Cyber Exercises at NATO includes building on, but neither duplicating nor complicating, existing exercises such as Cyber Coalition, Locked Shields, and the many national exercises. Reflections on exercises through the various lenses including NATO, various member nations, academia, and industry perspectives highlighted the sheer breadth of possible training objectives that cyber exercises should aim for - and the series of challenges that must be overcome to do so. Many of these challenges are not unique to cybersecurity; enhancing trust-building measures across NATO has been a discussion point for many years, as has the topic of aligning NATO and member nations' objectives when it comes to education and training. The external pace of change when it comes to cyber security and digital technologies is what makes the need for effective cyber exercise coordination particularly pressing.

With a growing almost-ubiquitous reliance on internet-connected technologies and tools throughout military infrastructure, it is crucial that relevant leaders, strategic, tactical and operational colleagues understand the implications of cybersecurity. This can be achieved through various forms of cyber exercises, undertakings that fit into NATO 2030 and the preparation for emerging challenges, as well as providing a mechanism to practice existing defence and response measures to today's threat landscape.