CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

TRUST IN CYBER EXERCISES: A VISION FOR NATO

Amy Ertan, CDR. Robert Buckles, Pilleriin Lillemets,
Lt. Col. Gry-Mona Nordli, and Lisa Catherina Schauss

7 March 2022

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

Contents

1. Introduction

Cyber defence is a team sport that requires collaboration and coordination between actors.

This report provides an argument for cyber exercises as a platform for increasing trust, and therefore collaboration within the domain, for NATO Allies.

Trust is essential to cyber defence, in and beyond NATO. Nations should be able to develop trust to share procedures, tactics, and best practices without exposing vulnerabilities. As NATO advances into this new decade, the members of the Alliance must find ways in which to share information and at the same time protect their national sovereignty. This is no easy task. It is well understood that Nations need to maintain their intellectual property and protect their exposure to threats. But Alliance members have to also realize that to venture further into collective defence in the cyberspace domain, they must be willing to share more of their tactics, techniques, and procedures with other Alliance members.

For too long has cyber defence been considered a clandestine area of operations. This report argues that sharing of information on cyberspace is no different than the Nations' behavior in other domains, and that there is a clear distinction between sharing valuable information on ones' capabilities versus recklessly exposing vulnerabilities. In the air domain, NATO Nations are familiar with the capabilities of their NATO Alliance members – speed, range, weapons systems, integrated contact tracking and fires, etc. In the maritime domain, Nations are familiar with ships weapons systems, range of operations, defence systems, radar ranges, etc. In these other domains Nations can learn to exercise warfare operations together and share capabilities without disclosing the full extent of their vulnerabilities.

So it must be the same in the cyberspace domain. Although Nations will surely choose not to share the full details of their capabilities within cyberspace, the Alliance can learn to operate together through cyberspace exercises. Well-constructed scenarios and exercise objectives will allow NATO and Nations to exercise warfare within the cyberspace domain while maintaining the sovereignty of their full capabilities.

The best environment to safely practice this sharing of information and capabilities is in exercises. This is a great arena for Nations not only to develop, but also share, new tactics and procedures while also refining information sharing methods. This is the environment for NATO Cyberspace Operations to practice coordinating collective defence – amongst NATO Entities and NATO Nations. NATO must establish exercise scenarios and environments in which NATO Entities and Nations are free to share their methods of collective defence without exposing their own national vulnerabilities. This is a delicate balance in which exercise planners have to be able to set incidents and events which challenge and fully engage the training audience.

Cyber defence is a team sport that requires collaboration and coordination between actors. This requires a culture in which exercise planners and training audience are comfortable to share information amongst the Alliance with the support of their home Nation and NATO Entities. The cyber defence community within NATO wants to improve the defence of the Alliance as a whole. In order for them to succeed, the political and military guidance must encourage a supportive environment in which cyberspace professionals can perform their duties.

Beyond developing and conducting exercises, NATO Entities and Nations have room for improvement in their sharing of lessons identified. Too often both NATO Entities and Nations are timid to share true lessons identified, lest they expose misperceived vulnerabilities. A shift in mindset is required through which leaders across the Alliance must encourage their cyber defence teams to be truthful in their reporting of lessons identified, without fear of reprimand. To know one's own weaknesses is the only way in which to improve and become more resilient. Nations must evaluate what is truly sensitive

information and consider releasing more when sharing their lessons identified. Additionally, NATO and the Alliance must carefully consider what information *must* be classified information, and where this is the case, ensure the information can be shared across the NATO information enterprise.

This report articulates NATO's current approach to cyber exercises and outlines several recommendations on an effective path forward relating to cultivating trust, engagement with allies, leveraging external expertise, and developing Lessons Learned advantages. This report builds on findings from an expert workshop held at the 13th International Conference on Cyber Conflict: Going Viral.

2. Context

> Establishing trust between Allies to achieve effective exercise and training within defensive Cyberspace Operations is already a major leap.

NATO has been conducting exercises since 1951. Today, NATO runs a number of exercises which either include cyber aspects or which focus specifically on cyber security and defence. With the planning process for each iteration often taking up to 18 months, NATO exercises are the culmination of diverse efforts from subject matter experts across and beyond the NATO Enterprise. Statistics from Locked Shields show that exercise planning and delivery exceeded 100,000 hours of effort. The resources dedicated to NATO exercises and training, including Cyber Operations, are immense - and for good reason. However, with resources limited both in terms of the skilled expertise required to design and coordinate a training exercise, and in terms of the limited pool of national participants who take time away from their national duties to take part. NATO exercises should be deliberately designed to fulfil training objectives in as streamlined and effective way as possible, reducing duplication, redundancy and inefficiency.

Focusing on training of cyber content highlights several ongoing discussion themes for NATO leadership. How does NATO best incorporate the cyberspace 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 does 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?

When discussing training and exercises within Cyberspace Operations, the question always arises of exercising offensive cyber in addition to cyber defence. Trusting others with information about the offensive capabilities a Nation controls might in some cases be even more sensitive than sharing own vulnerabilities. Although this is an interesting and relevant discussion, exercising offensive cyber will not be covered in this report. Taking it one step at the time, establishing trust between Allies to achieve effective exercise and training within defensive Cyberspace Operations is already a major leap.

As an organization, 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, the authors of this report engaged with experts across Allied Command Transformation, Supreme Headquarters Allied Powers Europe, NATO Communications and Information Agency and the NATO Cooperative Cyber Defence Center of Excellence. Engaging with NATO colleagues who are integral to the exercise design, development and delivery process, NATO policy-creators, as well as external colleagues revealed opportunities to leverage national, industry, and academic best practices. This document provides an overview of the status quo at NATO relating to the inclusion of cyber aspects into existing joint NATO exercises, as well as the delivery of effective cyber exercises. This report focuses primarily on NATO Members, with a reflection on benefits to increased engagement and greater information exchange beyond the Alliance, with NATO Partners and trusted external organisations.

3. Culture and Trust-building in NATO Cyber Exercises

> NATO must resolve the difference between cyberspace and other domains by re-baseline its level of trust.

Efforts to develop and maintain trust across the NATO Alliance are dependent on organizational and leadership cultures. Significant research has been published on the importance of building a culture of trust within an organisation. Many describe trust from a small-to-large approach: individual trust in others, trust in leadership, trust in a specific goal, and trust in the organisation's mission. Other approaches to developing trust include defining levels of trust; one might trust someone to return a book to the library for them but not to babysit their children, or one might trust an employee to deliver a task on time but not to keep sensitive company information secret.

When analysing trust within NATO, clearly the scope of trust expands multilaterally. It is understandable and common for Nations within the Alliance to trust some Nations more than others. Nations enter into bi-lateral and multi-lateral agreements and information sharing structures which allow a trust amongst them beyond that which NATO offers. Nations have natural biases given the capacities of other Nations in operational domains within NATO. And Nations have past and recent histories with other NATO Nations and Partners which cause them to adjust their level of trust with each other.

Nations in the Alliance behave in this same manner within the cyberspace domain. Often considered clandestine in its roots, the cyberspace domain is mired in behavior that yields barriers to information sharing. Cyberspace Operations originated from requirements of espionage and to sabotage. Even though recognised by NATO as a full operational domain since 2016 - with more traditional defensive and offensive mission sets - the cyberspace domain has yet to shed its mystique of secrecy. This leads to Alliance Nations and their cyber defence entities behaving in a less cooperative manner amongst themselves and Partners.

NATO must resolve this difference between cyberspace and other domains by re-baseline its level of trust. This can be done in three steps: 1) conduct an honest assessment of the level of trust within the NATO cyberspace domain today, 2) determine the required level of trust required within the cyberspace domain to operate optimally, understanding that full trust will never be reached, and 3) adjust culture within the Alliance and the domain to reach the desired level of trust.

Adjusting culture starts with individuals. NATO leadership must be honest unilaterally about where their level of trust is today, and where they want to go. Individuals within the Alliance must buy in to the new direction, and this requires clarity of effort. And finally, Nations must understand how much trust they give and are afforded within the cyberspace domain and determine if where they stand today truly benefits them and the Alliance.

According to the NATO 2021 Brussels Summit Communiqué, an important step towards assessing the current state of NATO Enterprise was taken with the establishment of the NATO Chief Information Officer's position. The role of the CIO is to enhance NATO's political-military coherence and situational awareness, both of which are indicators of trust between various stakeholders involved in NATO's cyber security. The CIO will create and overview the roles and responsibilities of those stakeholders, and hence help ensure future NATO cyber exercises address the right training audiences based on their realistic work roles. Having a clear understanding who should be responsible for what during the exercises helps to create more trust between the audiences, which transcends to real life situations on the job.

As Retired Admiral James Stavridis (former Supreme Allied Commander at NATO) wrote after the 2018 Trident Juncture exercise, "… exercises are an opportunity for the NATO and NATO Partner militaries to simply practice the art of war". There is no better place to begin adjusting NATO's culture of trust within the Cyberspace Domain of Operations than in exercises. The remainder of this report focuses on different areas of the cyberspace domain with respect to exercises.

4. Strategic and Political conditions for cyber exercises

There is a need for strategic guidance that clearly supports the measures needed for trust-building through exercises.

For the cyber exercise community to be able to deliver, build trust and integrate cyber into the overall family of NATO training and exercises, certain political and strategic pre-conditions must be met. Just as cyber exercises do not exist in a vacuum from the rest of NATO's exercises, cyberspace as a domain is not divided from the rest of the domains. Quite the contrary, cyberspace is intertwined with all other domains across the operational environment.

There is a need for strategic guidance that clearly supports the measures needed for trust-building through exercises. Never before has there been better momentum for developing such in NATO. The Heads of State and Government will approve the new NATO's Strategic Concept in Madrid in the summer of 2022, which will subsequently set a number of follow-on activities in motion. The new Concept is set to reflect the new strategic environment in which the Alliance is operating in, including the ever more relevant role of cyberspace as a Domain of Operations. It is time for NATO to see cyber defence in the context of the Alliance's overall deterrence and defence, making it one of the many tools in NATO's toolbox instead of a separate, often misunderstood, and mystified technical issue. Reflecting this fundamental change in the follow-on plans and policies will allow future NATO exercises to better reflect the cyber domain realistically, as a part of the overall, multi-domain, operational environment.

Political commitment to include trusted partners is essential. In cyberspace more than in any other domain, the Alliance is dependent of building a network of trust that reaches beyond its borders, to increase situational awareness on potential malicious activities across the borderless cyberspace. As repeatedly pointed out in this report, building the required level of trust in cyberspace is essential, and it takes time and commitment to create such relations.

In June 2021, NATO Allies affirmed their commitment through the Brussels Summit Communiqué to "further seek to develop mutually beneficial and effective partnerships as appropriate, including with partner countries, international organisations, industry, and academia, furthering our efforts to enhance international stability in cyberspace." If NATO truly wishes to build trust with its partners, practical commitment from the Alliance's side is required. In more practical terms, this would mean including partners into NATO's exercises, where applicable, on a permanent, rather than case-by-case basis. This would enable the trusted partners to be able to plan for participation well in advance and hence bring more added value. Additionally, the Exercise planners would be able to develop necessary storylines for partner inclusion with a long-term, instead of one-year view in mind, hence increasing the quality of those products.

5. The Challenge of Trust at NATO

> As NATO fulfils its core tasks through operations it is imperative that cyber considerations are incorporated.

Trust can be developed when there is a common language and understanding between groups. One current challenge facing exercise designers and coordinators is the general lack of understanding of the operational impact of cyber effects in the military context. Senior leaders in military and defence spheres don't necessarily understand what vulnerabilities are, or how a cyber effect may have direct or indirect implications in and beyond the conflict environment. As NATO fulfils its core tasks through operations it is imperative that cyber considerations are incorporated, mirroring real-world conditions in which operations are almost ubiquitously reliant on digital and internet-connected infrastructure.

Cyber considerations must become a natural part of any exercise, and not only silo'd into separate exercises. Exercising in this way offers a safe environment to develop trust though gradually developing the understanding of cyber effects across wider leadership. The common language and understanding also goes both ways and cyber experts must understand the wider context of conflict in which cyber is often one tool in the state defence toolbox. To achieve effective integration of cyber aspects into operations, the cyberspace domain should not be treated as more special than it is. Education and training on cyber and joint exercises must recognize the nuances of the broader landscape and how different domains interact and develop a shared understanding based on this.

Addressing the current lack of understanding into cyber means recognising the difficulty of translating technical data about cyber-attacks into meaningful information for decision-makers. This communicative 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 and crisis management, while at the operational level, the focus is on C2 and situational awareness. At the tactical level, exercises are more about sharing tactics, playbooks, and incident management. More work is needed to understand these roles/responsibilities.

Developing this trust and communication also means having the right personnel to make sense of the environment. 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. The Alliance needs to develop collaboration and communication skills. The team needs to combine multiple roles, and they need to collaborate effectively.

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 does the Alliance measure success in training individuals and collectives? To have successful exercises, NATO must ensure training objectives are correct.

One way to better integrate NATO and national training would be through more extensive use of cyber ranges. To integrate in this way, a NATO cyber range is not sufficient by itself, The NATO cyber range needs to be supplemented with national cyber ranges, with opportunities to link national and NATO functions, capabilities, and exercises. For example, data from national cyber ranges could be used to identify training gaps at national levels to be addressed through NATO individual training and exercises.

6. Sharing Lessons Learned

> The exercise is not over until the maintenance is done, and this culture must also be transferred to the Lessons Learned process.

The most important outcome of most exercises are the lessons learned drawn from what is experienced during the planning, preparations and execution of the exercise. The idea of sharing lessons learned across organisations and nations is to save time and recourses by learning from the mistakes others have made or adopting the successes of other. Most organisations across public and private environments have some sort of process for identifying Lessons and implementing the remedial actions, this is how the organisations can learn and improve. For NATO, it is essential that NATO entities and national militaries are able to share relevant training information. Achieving a trusted environment where exercise audiences feel comfortable sharing - and ingesting - lessons learned material means adjusting existing several challenges with the status quo of limited information exchange.

While we discuss several common challenges below, it is important to note that the obstacles to effective information sharing differ when sharing *between*, and *beyond*, NATO Members.

Sharing *outside* the Alliance with Partners within 7NNN as well as other Partner Programs is a separate issue, which will shortly be summed in this section.

There are a number of non-NATO Nations which could contribute to and benefit heavily from NATO discussions, exercises or operations. These Nations, formally designated as Partners (/define), have already closely worked or cooperated with NATO in different ways but are still often excluded by default to sensitive discussions and Lessons Learned material due to NATO Security Policy. As the NATO Lesson Learned Portal (NLLP) is already considered an underused tool within NATO, it is probably even less known among NATO Partners. Even though, according to 'NATO JALLC's Procedure to Access the NATO Lessons Learned Portal', it is possible for Partner Nations to get access points to this portal, at least on NU WAN. Formally, a stronger inclusion of Partners in the Lessons Learned process could be possible.

Information sharing mechanisms such as Malware Information Sharing Platform (MISP), a platform facilitating information exchange on malware, have shown that such important content can be shared with non-Members in a structured fashion. Where NATO Partners have valuable information that would benefit the Alliance, or vice versa, there is a need for mechanisms that facilitate this exchange, as an issue of mutual interest and a sign of trust.

Whether this means implementing new mechanisms, repurposing of existing mechanisms to allow for greater partner engagement, or encouragement of underutilized and already existing mechanisms or platforms that partners could use, should be a leadership decision.

The remainder of this report will focus on sharing within NATO.

It has been observed that post-exercise, Nations usually do not want to share Lessons Learned / Lessons Identified especially when any disclosure would reveal their team's shortcomings or vulnerabilities experienced through an exercise. This is an obvious approach; no Nation wants to reveal information on their vulnerabilities. The perception by participants is that by sharing the Observations, Lessons Identified, Lessons Learned or best practices one also shares own failures and vulnerabilities - and in the cyberspace domain audiences are particularly protective of their vulnerabilities as this is easily exploited by our adversaries. Nonetheless, this hesitation may mean under-sharing of information, including Lessons Learned that would not reveal such sensitive content, but benefit other Parties

involved. We view the sharing of vulnerabilities as distinct to sharing Lessons Learned – with opportunities to share relevant TTPs, without specifically sharing vulnerabilities. This points to the larger challenge of trust, and trusting other nations, across the NATO structure of entities and nations.

There are opportunities to build trust through the sharing of Lessons Identified/Lessons Learned. NATO has a strong Lessons Learned process that exceeds those in place for some states. In addition to identifying areas for improvements the process has also been used to identify aspects that worked well, enabling future exercise iterations to repeat successful characteristics and make any potential corrections. This trust-building doesn't necessarily require the disclosure of vulnerabilities, with one safe approach being the sharing 'best practices'. Sharing observations or best practices makes it possible to learn from one another without revealing secrets or weaknesses.

There are mechanisms available for such information-sharing. The Joint Analysis and Lessons Learnt Centre (JALLC) is the lead NATO body for Lessons Learned and Identified across NATO:

> *"The JALLC's Mission is to support Alliance-wide implementation and sustainment of NATO's Lessons Learned policy through monitoring and supervising the NATO Lessons Learned Process within the NATO Command Structure and other NATO bodies. It is the lead agent for the collection and sharing of lessons, accomplished through active content management of the NATO Lessons Learned Portal, Joint Analysis (as an integral part of the Lessons Learned Process) and outreach to allies and partners".*
>
> *JALLC Homepage,* https://www.jallc.nato.int/.

The NATO Lessons Learned Portal (NLLP) is the centralised hub for all lessons learned information, including observations, Lessons Identified, best practices and completed Lessoned Learned, and takes submissions from all NATO entities, NATO nations and Partner Nations to some extent. Within the NLLP there is an existing Cyber Defence Community of Interest (CoI) where sharing lessons relevant to the cyber community is possible. This is a little known and heavily underutilised tool by the NATO cyber community, with the NLLP being used for other domains to a relatively greater extent.

As a CoI, we raise the question of how best to promote this tool or any preferable mechanism. The Cyber Defence CoI Portal offers the chance to incorporate material including exercise reports, training analysis, identified best practices, and a number of other valuable aspects that do not necessarily require states to disclose sensitive information, or information on their vulnerabilities. However, in order to live up to its potential, the portal must actually be used with participants submitting inputs to a much greater degree.

There is awareness of these broader within the Lessons Learned community as attendees of the 2021 NATO Lessons Learned Conference highlighted the importance of collecting and exploiting Lessons Learned content (as highlighted in the NATO Lessons Learned Conference 2021 Report, p21). With the recognition in place, this report recommends several possible actionable goals relating to lessons learned. First, there should be an agreement on how Lessons Learned are managed across the cyber community, particularly in post-exercise analysis. One way to achieve this would be to establish a Lessons Learned Cyberspace Forum as an extension to the Cyberspace Operations Education and Training Annual Discipline Conference. Second, any mechanisms should be able to capture Observations and Lessons Learned not just from cyber exercises but also from cyber-related observations in joint exercises. Finally, the emphasis should not be limited to encouraging participants to share lessons, but also encourage participants to draw from the observations, Lessons Identified or Lessons Learned from others, benefiting from the greater information available.

A rule of thumb in any military exercise is that the exercise is not over until the maintenance is done, and this culture must also be transferred to the Lessons Learned process. Why do we even exercise if it's not to learn something? These lessons must be documented for future use and also shared with

others that might come across the same challenges. When planning an exercise the first step is always to look at the lessons identified from previous exercises, including Lessons made across the Alliance will improve the starting point. The NLLP is the single point of sharing lessons learned in NATO and must be promoted to a greater extent in the Cyberspace Operations community.
Use of any information sharing portal will require developments in trust across participant teams and the execution of this reports recommendations on culture and leadership will go some way to encouraging greater sharing of Lessons Learned and related material. The NATO Lessons Learned process is taught and practiced in all domains, as the process itself is generic and can be applied for any kind of operation, exercise or training. Cyber is not, and should not be, an exception.

7. Benefiting from expert insights: Industry and Academia

NATO has numerous trusted partners both within industry and across academia.

NATO cannot develop effective exercises in isolation and without the contributions from the public and private sector, and from academic. As well as potential service provision provided by industry partners, cooperation with trusted academic and industry networks enables NATO to benefit from the skilled expertise from these sectors, as well as to cutting innovation and analysis that complements NATO's internal activity. Many civilian entities are frequently engaged in cyberspace operations and will have valuable experience to contribute. Furthermore many will have employed ex-military personnel who can contribute a unique set of knowledge having operated across military and civilian organisations, which may again prove valuable in highlighting new avenues for exercise design, including through shaping capability-development opportunities. In this way, inclusion of civilian expertise may help increase defence in depth, expanding below the NATO "bubble".

The expert workshop reflected that while the military has a history of benefiting from industry and academic cooperation, traditional military secrecy and mistrust towards outsiders prevent military organisations from getting the full value of learning from partners. While current events have demonstrated that conflicts are, and will likely continue to be, hybrid, the community of experts' view was that this is often not reflected in NATO cyber exercises. NATO and national militaries still 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. In order to gain full value from engagement with industry and academia, it is argued that military organisations 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.

There is work underway in this regard. While there is room for improvement when it comes to cyber exercises, NATO has been clear about the need to engage with non-military partners more broadly (with mechanisms including the NATO Industry Cyber Partnership, of the Science for Peace and Security programmes). NATO has demonstrated a willingness and commitment to work with industry as part of a broader technology-related agenda: the NATO Innovation Fund, and the Defence Innovation Accelerator for the North Atlantic (DIANA)

NATO has numerous trusted partners both within industry and across academia. In early 2021 a $42bn contract was secured with Thales for deployable communications and information systems (DCIS), as well as agreement for Thales to provide deployable defence cloud capabilities ('Nexium Defence Cloud'). NATO relies on industry provision and support of cyber defence infrastructure. NATO has numerous mechanisms designed to increase cooperation with private entities, including the NATO Industry Forum, NATO Industrial Advisory Group. There is a NATO Framework for Industry Engagement (2013). Such initiatives only highlight NATO's commitment to greater industry collaboration as highlighted by Secretary General Jens Stoltenberg in November 2021.

> Through the NATO Industry Cyber Partnership (NICP), NATO and its Allies are working to reinforce their relationships with industry. This partnership includes NATO Entities, national Computer Emergency Response Teams (CERTs) and NATO member countries' industry representatives. Information-sharing activities, exercises, training and education, and multinational Smart Defence projects are just a few examples of areas in which NATO and industry have been working together.
>
> *NATO - Cyber Defence Homepage*

Increasingly this cooperation and collaboration can be seen in NATO exercises. These instances should be expanded to realize the full benefits of working with approved external partners and vendors. Incremental expansion of public-private cooperation allows NATO to continue to remain caution while gradually improving connections with industry (and where appropriate) or academic partners. In practice, this means acknowledging where selected organisations have already been approved to work with the NATO Enterprise, or for equivalent projects with national efforts, and using this trust as a starting point for future collaboration. By focusing on expanding public-private participation by scaling up the engagement with existing partners, NATO exercises do not need to 'start from scratch' to bring in tools and expertise and can leverage assurance efforts already completed elsewhere.

Finally, external engagement does not have to be limited to corporate contracts with trusted industry vendors. Academic partners can offer expertise and resources including software and hardware provision, as well as evidence-based advice based on robust research.

8. Recommendations

In order to best develop the trust required to design and run effective NATO cyber and joint exercises with cyber injects, colleagues who are responsible for developing and delivering cyber (or joint cyber) exercises should:

8.1 Culture, Trust, and Strategic Conditions

- NATO and Allies should review its methods for sharing existing and new tactics and procedures while also refining information sharing methods.
- NATO should encourage exercise planners to be able to set incidents and events which encourage greater information sharing in order to challenge and fully engage the training audience.
- NATO Nations should evaluate what is truly sensitive information and consider releasing more when sharing their best practices and lessons identified. Additionally, NATO and the Alliance must carefully consider what information *must* be classified information, and where this is the case, ensure the information is able to be shared across the NATO information enterprise.
- NATO and Nations should invite as training audience multidisciplinary specialists with operational, logistic, and intelligence expertise to broaden the operational understanding of the characteristics of a domain built on technology.
- NATO Enterprise Chief Information Officer should assess the maturity of the organization in terms of readiness to respond to cyber threats. Identifying also the aspects in which the lack of trust between various stakeholders is hampering NATO's ability to respond, this assessment could be used as a basis for reviewing the participation and roles of NATO Enterprise cyber stakeholders in Exercises.
- Strategic and operational leadership should ensure that the training objectives established for various training audiences reflect those audiences' actual roles and responsibilities, and enable different stakeholders to build trust through cooperation within NATO cyberspace exercises.
- Resolve difference between cyberspace and other domains by re-baseline its level of trust. Specifically:
    - Conduct an honest assessment of the level of trust within the NATO cyberspace domain today
    - Determine the required level of trust required within the cyberspace domain to operate optimally, understanding that full trust will never be reached
    - Adjust culture within the Alliance and cyberspace domain to reach the desired level of trust

8.2 Increase genuine engagement with Lessons Learned processes

- NATO should encourage information sharing with the emphasis that sharing Lessons Learned-related material does not require the disclosure of sensitive material relating to capabilities or identified shortcomings. Facilitating the sharing of post-exercise best practices is an actionable first step to developing this trust and setting a precedent for an active NATO Lessons Learned Portal.
- NATO should insist the JALLC be an integrated part of each cyberspace exercise Lessons Learned process to encourage greater sharing of information during and after the exercise execution. This could apply to exercises including but not limited to Cyber Coalition, Locked Shields and Crossed Swords.

- NATO should establish a Lessons Learned Cyber Forum as an extension to the Cyberspace Operations Education and Training Annual Discipline Conference. Mechanisms of this forum should be able to capture observations and Lessons learned not just from cyber exercises but also from cyber-related observations in joint exercises. The emphasis should not be limited to encouraging participants to share lessons, but also encourage participants to draw from the Observations, Lessons Identified or Lessons Learned from others, benefiting from the greater information available.

8.3 Streamline partner participation

NATO should modification of the approval process for Partner Nation participation in NATO Cyberspace Collective Defence Exercises to match other Domains of Operation:

- Currently, Partner Nation participation in NATO exercises requires NAC approval through the Military Training and Exercise Program Open to Partners [MTEP OTP] process. Partner Nations are recommended by the Military Committee for approval in specific NATO exercises. The MTEP OTP follows a five-year plan.
- Article Five and cyberspace exercises require annual, case-by-case approval by the NAC. This places NAC approval of cyberspace exercise participants on par with Article Five exercises, a level of scrutiny for which no other Domain of Operation is subjected. For cyberspace domain exercises, this creates a barrier to entry for Partner Nation participation greater than that of other domains. It hinders long-term planning on both the cyberspace exercise planners and the Partner Nations.
- The Cyberspace Domain of Operations has been recognised for over five years now by NATO. Aligned with similar efforts to manage the cyberspace domain as NATO does other domains, NATO should adjust its Partner Nation approval process to match that of the other domains. This would greatly improve cooperation with Partner Nations, allow for long term planning, and lend to a greater development of trust between the Alliance and Partner Nations.

8.4 Deepen industry partnerships

NATO should realize the full benefits of external resources and expertise by expanding its engagement with industry partners:

- Foremost NATO should focus on deepening existing relationships with trusted third party suppliers such as exercise platform providers. This allows for increased trust with approved partners who have already met sufficient assurance requirements and avoids 'starting from scratch' in terms of trust and supplier onboarding.
- NATO should *incrementally* expand engagement with external partners and vendors. A 'slow and steady' approach to greater collaboration allows NATO to benefit from external expertise without sacrificing any supply risk assurances.
- NATO should apply the same principles with academic partners. Locked Shields is one example in which the exercise benefits from input and live-event support from Tallinn University of Technology.

9. Further opportunities for inclusion of cyber aspects into NATO exercises:

This report has focused on the key theme of trust. There are a range of other themes that require attention, and we hope that this report helps develop the discussion around effect exercise design particularly relating to the cyber design. Some of the key themes that should be explored are: Effective Exercise design: achieving the right balance between realism and effective learning; encouraging appropriate risk-taking in exercises without punishing failure; engaging participants while developing their capabilities and expertise. Aligning National vs NATO training objectives. While national and NATO exercises will hold different priorities there are opportunities to leverage the overlap to minimise duplication and achieve better integration of NATO capabilities. Integrating cyber into joint exercises. 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.

10. Conclusion

This report presents the case that greater trust between NATO Nations and Partners holds a number of advantages for cyber exercises, many of which are intuitive. Greater trust levels between Nations will increase the strength of NATO's collective defence capabilities to allow the Alliance to maintain a united front against threats - many of which will increasingly be technological in nature. Exercising provides a unique platform for militaries and national defence practitioners to develop this trust in a safe environment, practicing the collaboration and rapid response that is required when facing real-world cyberattacks.

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. Reflecting on exercises through the various lenses including NATO, various Member Nations, academia, and industry perspectives highlight 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 cyber defence; 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 cyber defence. 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.