Information & Security: An International Journal

Konrad Wrona et al., vol.36, 2017 https://doi.org/10.11610/isij.3603

CYBERSECURITY INNOVATION IN NATO: LESSONS LEARNED AND RECOMMENDATIONS

Konrad WRONA, Tamsin MOYE, Philippe LAGADEC, Michael STREET, Peter LENK, and Frederic JORDAN

Abstract: In the ever-increasing pace of technological development and the emergence of new stateless adversaries and threat vectors, the traditional NATO approach to the technical capability development struggles to address the emerging security challenges in cyberspace. In order to mitigate this situation, we describe an incubator framework, which provides a physical and virtual environment enabling industry, in particular small and medium sized enterprises, science and technology organizations, academia, and national defence labs, to collaborate on innovation projects on the basis of either voluntary, nationally funded, or NATO commonly funded contributions. The proposed incubator framework has been practically validated and technical results have confirmed the feasibility as well as the benefits of setting up a cyber incubator within NATO. This disruptive approach to capability development requires the updating of several internal processes and procedures and the adoption of a new innovation-friendly and risk-tolerant organizational culture within the Organization. We describe the main lessons learned from our experiment and the recommendations regarding required changes to the internal and external NATO processes and procedures.

Keywords: NATO Industry Cyber Partnership, Cybersecurity Innovation, Data Fusion, Mobile Security, Situational Awareness.

1 Introduction

1.1 Motivation

The ever-increasing pace of technological development, as well as the emergence of new stateless adversaries and threat vectors and means, the traditional NATO approach to the technical capability development struggles to address the security challenges emerging in cyberspace. Although working in close relationships with existing NATO industry partners offers a well-understood and tested way for incremental improvement and *doing what we do but better*, the existing NATO innovation ecosystem and collaboration procedures do not provide an effective route to devel-

oping radically different approaches and accessing significantly different sets of knowledge required to efficiently face the emerging cybersecurity challenges. We need to develop new ways of generating ideas, allocating resources to projects, and identifying and working with partner organizations to provide an efficient and effective way to address the disruptive challenges faced by NATO in the cyberspace.

In this paper, we present the lessons learned and recommendations from a pilot project supporting the implementation of a NATO *cybersecurity incubator*. The project was executed by the NCI Agency between January and September 2015.

1.2 Approach

The main objective of the cybersecurity incubator pilot project was to assess the viability of NATO taking a new collaborative approach with industry, academia, and government research entities to achieve some of its goals related to innovation and transformation within NATO.

The initiation of the pilot project was supported by the following four stage process:

1. Idea generation and call for proposals;
2. Selection;
3. Cooperation, development and testing;
4. Exploitation.

The pilot project was limited to the definition of challenges and investigation of innovative solutions in three focus areas, which had been identified as areas where the Alliance urgently requires cyber defence solutions:

- Cybersecurity data fusion;
- Agile cyber defence situational awareness;
- Mobile security.

A description of the specific technical challenges associated with each focus area is provided in Section 2.

1.3 Objectives

The core objective of the incubator activity was to achieve the maximum results possible within a limited timeframe by introducing quick and agile collaboration mechanisms that will lead to creative and innovative solutions to the problem statements describing the three focus areas mentioned above. The expected deliverables, communicated to prospect participants, were the same for all of the focus areas and included:

- Hardware and/or software demonstrator, usable for further validation and testing;
- Concise design and operational documentation of the demonstrator;
- Documentation of test scenarios, test data and test results.

The demonstrator could have been provided in one of two forms:

1. As software including open-source components and custom components, both in source and compiled forms, configuration files, scripts and source text for any customization, or
2. As a fully functional virtual machine(s) including configuration and test data that can be used to run the demonstration scenarios.

1.4 Timeline

The project started in January 2015 with an internal coordination and selection of the initial focus areas. From the beginning the focus was on agility and quick progress. Thus, shortly thereafter, in February, a kick-off event was hosted at The Hague Security Delta (HSD) Campus. The event was attended by nearly 100 delegates from industry and academia. During this meeting, the NCI Agency presented the objectives of the pilot project, the technical challenges under consideration as well as the proposed collaboration framework.

As a follow-up, industry and academia were invited to present their technical solution at a workshop also hosted at the HSD Campus in March 2015. Three (one per focus area) 2-hour sessions allowed each organization an 8-minute slot to present their ideas, and five minutes to answer questions and receive feedback prior to final proposal submission. Organizations that had requested their proposals to be discussed in full confidentiality were invited to present their solutions on the premises of the NCI Agency.

The deadline for the submission of the final proposals was a week later. It was followed by a rapid proposal evaluation phase of two weeks, during which selected technical experts from the NCIA cybersecurity and innovation groups were assembled to evaluate the proposals and make recommendations on those to take forward. Coordination with the NATO Allied Command Transformation (ACT) ensured alignment of these recommendations with the NATO transformation activities.

At the end of March, the projects were initiated with the selected partners. The projects were completed by end of August 2015 and the results were successfully presented at the annual NATO cybersecurity symposium (NIAS) in September 2015.

This quick pace of execution—nine months from starting planning of the activities to finalizing the results—was only possible thanks to enthusiasm and dedication of the

technical and support staff from both NATO and the partner organizations participating in the innovation projects. This unusual speed has also the benefit of exposing many inadequate processes and procedures used within NATO in the context of the external collaboration.

2 Focus Areas

Below we introduce in more detail the three innovation focus areas, which were targeted by the incubator.

2.1 Cybersecurity Data Fusion

Cybersecurity data fusion [1,2] requires asset, threat, vulnerability and incident information collected from several sources, both manually created and automatically generated, from both internal sources (e.g. network scans, asset databases) and external sources (e.g. vulnerability reference information) to be combined in useful ways to derive high quality information to support risk-based decision-making. This is often challenging for organizations − the data is often conflicting, incomplete and of low quality.

The objectives of this activity were to develop and demonstrate tools, which can be used to track the pedigree of data [3] and compute metrics that measure the data quality, including its reliability, and at the same time extract additional high quality intelligence by fusing the data.

2.2 Agile Cyber Defence Situational Awareness

Cyber defence situational awareness (CDSA) [4,5] requires a broad range of information and data items coming from various sources that need to be collected, fused, analysed and visualized. The data sources, the data formats, the analysis algorithms and the visualizations need to be continuously adapted to the changing environment, the evolution of systems and networks, and the rapidly evolving threats. It is therefore necessary to explore agile and flexible solutions to build CDSA systems.

The objective of this activity was to design and build a demonstrator of an agile CDSA system, based on technologies providing data storage, indexing, searching and visualization with an agile data model (e.g. NoSQL [6]) and flexible visualization that allows users to build custom views from queries. The demonstrator was to be preferably built using freely available open-source software such as Elasticsearch/ Kibana [7] or similar, so that it could be reused without restrictions by NATO and its partners.

The demonstrators were implemented according to a conceptual data model [8,9] that had been provided by NATO at the beginning of the activity. They were tested using scenarios and test data provided by NATO.

2.3 Mobile Security

Mobile devices are playing increasingly important roles in the processing of information. However, in addition to increased convenience, mobile technology also introduces many new challenges. Due to the limitation on size, weight, and power consumption, mobile devices provide typically less physical protection than desktop devices traditionally used within NATO. At the same time, due to the way they are used, mobile devices are more susceptible to loss or theft by an adversary. Thus, it is important that the additional risk related to processing and storage of information in mobile devices is properly taken into account when defining and enforcing access control policies.

In many cases, mobile devices may be privately owned by NATO employees, in accordance with a Bring-Your-Own-Device (BYOD) concept,[10] or non-NATO entities, e.g. NATO partners such as non-NATO nations, non-governmental organizations, or other international organizations. In such cases, the configuration of the device might be only partially controlled by NATO. A mechanism for enforcement of applicable NATO policies at the device needs to be devised.

Finally, the variety of sensors included in modern smart phones and tablets, as well as the ability to collect location information, introduce new attack vectors and possible side and covert channels, which need to be taken into account.

Despite all of the above security challenges, mobile devices also introduce potential benefits for security. Most of the devices include some type of trusted computing platform and support different types of user authentication. Mobile devices can also provide context information about the user and his location, which can be used to design and enforce complex and fine-grained security policies.

The solicited project proposals were to address at least one of the following objectives:

1. Providing a prototype and validation of enforcement of complex access control policies for mobile devices, including support for different security domains, e.g. various NATO classification levels or BYOD;

2. Providing a prototype and validation of innovative applications enabling use of mobile technology to improve the cybersecurity posture of NATO in various areas.

3 Sample of Project Results

In order to illustrate the scale and character of the projects executed within the incubator, we discuss below briefly some of the innovation projects executed in the mobile security focus area. Four projects have been executed in this area, related to the

BYOD concept, behavioural authentication, assisted labelling of information, and use of post-quantum cryptography on mobile devices. We summarize the results of the first three of these projects below.

3.1 BYODroid

Smart devices are becoming more and more ubiquitous in everyday life. Their connectivity allows complex interactions with nearby objects and provides continuous access to the Internet of services. They are powerful and flexible instruments for many working environments. Thus, many organizations are interested in establishing a BYOD policy is respect to the use of privately owned smart devices at their premises or for work purposes. BYOD security implications must be evaluated carefully. Smart devices have advanced hardware and software capabilities, and if they have access to corporate facilities they can be used to steal sensitive data through malware applications or they can affect the behaviour of the ICT infrastructure by carrying out sophisticated cyber attacks. Supporting BYOD while providing security guarantees is currently an open issue that is being addressed by both industry and academia. Most existing commercial BYOD security solutions consist of mobile device management (MDM) systems. The security controls provided by a MDM solution typically target the device behaviour as a whole, for instance by enforcing a black list of undesirable applications. But these controls are often too coarse-grained to capture the actual security policy of a complex organization. BYODroid was proposed as a technology that allows automatic assessment of whether or not applications installed on a mobile device comply with the security policy of an organization.[11] The used policy language is expressed through a specification language that is expressive enough to capture the policies of real organizations.

Owing to the sensitivity of the managed resources, the NCI Agency infrastructure is subject to strict rules and behavioural policies that employees as well as visitors must adhere to. The use of mobile devices such as smartphones is restricted and, in some cases, prohibited. During the project two goals were pursued. The first was to evaluate the applicability of the BYODroid policy framework to the NCI Agency security rules for mobile devices. We started by processing existing documentation and security guidelines in order to extract a BYOD policy. This process involved active sessions with the NCI Agency security experts, in which the security rules were refined and precisely formulated. This allowed specification of an unclassified test policy covering several pertinent aspects of the security-relevant operations that a mobile device can carry out within the NCI Agency infrastructure. The second goal was to deploy the BYODroid support inside the NCI Agency ICT perimeter. This activity required an extension of BYODroid with extra components for authentication and authorization of the users. In particular, a role-based policy management system had

been added, which allows the security administrator to specify different policies for different roles. Users are assigned to one or more roles and roles can inherit existing security policies from a parent, super-role. The actual policy that a user is subject to is obtained as the conjunction of the involved policies.[12]

3.2 Behavioural Authentication

The search for new authentication methods to replace passwords for modern mobile devices such as smartphones and tablets has attracted a substantial interest in recent years. As a result, several new behavioural biometric schemes have been proposed. Most of these schemes, however, are uni-modal. Within the innovation project we have investigated a new bi-modal behavioural biometric solution for user authentication, called *Hold & Sign*. The proposed mechanism takes into account micro-movements of a phone and movements of the user's finger during writing or signing on the touchscreen. More specifically, it profiles a user based on how he holds the phone and based on the characteristics of the points being pressed on the touchscreen, and not the produced signature image. Although typing a PIN might seem to be easier than writing something on the touchscreen, a PIN can be forgotten, whereas most users remember their own name. Moreover, launching shoulder surfing and smudge attacks to steal PINs and passwords is relatively easy. In our method, even if an attacker knows what is being written, access is still denied because he cannot mimic the phone movements of the legitimate user.

Hold & Sign offers two advantages over traditional mechanisms. Firstly, a user can write his own name in an unconstrained way with a finger on the smartphone's touchscreen, which makes memorability and repetition easier. There is no need to remember a password/pattern and no need to keep them secret, thus eliminating the problem of sharing and stolen passwords. Also, it is easy to integrate and implement in most modern smartphones without the need for additional hardware. *Hold & Sign* can be used as a stand-alone method or can be used in conjunction with other well-established mechanisms for additional security. Since signature-based authentication is already deployed for user identification and it is also very common to use finger movements for navigating documents, e.g. web pages, photo albums, messages, etc., we expect our solution to receive positive user acceptance. More detailed discussion of the behavioural authentication concept and of the project results is available in other recent publications.[13,14,15]

3.3 Intelligent Classification

The intelligent classifier experiment was focused on examining whether the machine learning techniques [16,17,18] can be used as part of the automated classification techniques that NATO is currently exploring in the context of object-level protection.

In the intelligent classifier approach, the classifier makes use of statistical information about the appearance of words in a document to identify key patterns (called small worlds) and, subsequently, a machine learning system based on artificial intelligence is taught to categorize documents by these small worlds. A policy analyser is used to determine, based on the identified category, how the document should be handled and may inform, advise or enforce any decision, as well as log the outcome. A pilot study of the classifier in relation to NATO documents was carried out. The classifier took a sample of (now de-classified) NATO documents from the NATO Archive to determine if the Helmholtz classifier [17] can categorize them to an acceptable degree of accuracy.

The aim of the demonstrator was to take a large set of existing documents and convert them (from searchable PDF images) into text format so that the classifier could be applied. Depending on the operational environment different minimum values of classification accuracy A_c were required. If the machine learning approach is used in a scenario in which the proposed classification level is reviewed by a human, an $A_c >$ 95 % may be acceptable, whereas in a fully automated classification environment handling documents of potential high sensitivity, an $A_c > 99.9$ % may be required.

The data set used was a large sample of NATO de-classified documents from the 1950s available in the NATO Archives. A commercial OCR conversion program was used to render the documents into text form. A sample of documents from a homogeneous operational area (military committees) was identified for training purposes. This was divided into training, validation and test sets on the basis of the documents original classification. It was assumed that the original classification was sufficiently accurate to give a low probability of error resulting from initial misclassification.

Although the classification accuracy Ac ≈ 80% achieved during the experiment was well below the required operational accuracy, the results from the experiment were promising. First, the low Ac was to a large extent a result of the limitations imposed by the quality of the available data set and would be significantly improved if a fully machine-readable data set were used. Furthermore, we were able to demonstrate that the process does not require prohibitive computational resources, in fact it can even be executed on a mobile terminal. Finally, we demonstrated that correct classification did not depend on the existence of security tags in the document (such as top secret or unclassified) but made use of the entire contents of the document to provide pattern recognition at a semantic level. More detailed discussion of the project results can be found in our recently published work.[19]

4 Lessons Learned and Recommendations

One of the important goals of the cybersecurity incubator project was to gather initial experience with performing rapid innovation within NATO and with new ways of working with our industrial and academic partners. Many lessons were learned which we believe might be useful for other international and governmental organizations contemplating involvement in the innovation activities in some rapidly developing areas of interest such as cybersecurity.

The lessons learned and recommendations can be divided into five main areas, and include the overall concept; coordination and management; communication and collaboration; infrastructure; and legal considerations. All these areas are discussed in more details in the sections below.

4.1 Overall Concept

4.1.1 Incubator Focus

In order to maximize the chances of success, it was found that the number of focus areas was too large and that the individual topic definitions were perceived by the applicants as too broad. Informal discussion with industry indicated that when they conduct similar activities, even in a single well-defined area, they expect that only about one in ten projects will result in a successful capability in production. Therefore, in the future, we would anticipate having individual incubation activities, with potentially several parallel projects, focused on just one topic area and the topic described in terms of a detailed and well-defined *problem statement*. This approach would also minimize a risk that some broad concepts, e.g. Big Data, are misread, attracting a lot of proposals focusing on specific issues without relevance to NATO. Furthermore, the use of a common terminology as well as a common understanding of the NATO context are two key elements for an effective dialogue with industry and academia. We believe that this more specific focus and precise formulation of problem statements, combined with a well-structured selection process, will maximize the opportunities for successful outcomes.

4.1.2 Incubator Applicability

Although the incubator was conducted in support of the cyber domain, the concept has applicability across a wider set of ICT domains of interest to NATO. Although the next few incubators that the NCI Agency is currently considering would almost certainly be concerned with problems identified in the cyber world, in the future the concepts may also be extended to other problems across a wider set of topics of interest.

4.1.3 Flash-to-Bang Approach

We incubate to define requirements based on the problem statement while at the same time developing or adapting potential solutions to those problems. This is an important concept, that is, the simultaneity of the development of a deeper understanding of the problem while at the same time developing an instance of a solution. This is fundamental and is the strength of the approach as a way to closing the ever-widening gap between the advancement of technology and threat capabilities. It was realized that this pilot activity was only focused on the first part of the problem. What the incubator did not consider is a way to pull the solutions through the next stage, and into production. This second step is considered in more detail in Section 5.1.

4.1.4 Fail Fast

One of the terms, that has come into common usage when dealing with innovation is *Fail Fast*, meaning that an organization should not be scared to have failures and in fact celebrate these, as long as something is learned. The incubator framework gives a perfect vehicle for this as there are several off-ramps inherent in the process. An easy point to terminate ideas that are not proving entirely satisfactory is at the end of the incubation phase, prior to putting things into production. This means that the risk that the Agency is assuming is limited to only the limited incubation funding available. It would probably also be wise to introduce an earlier *gate*, perhaps at the mid-point of the incubation where ideas that are not showing value could also be terminated.

4.1.5 Diversity

Innovation is expedited through diversity. A variety of viewpoints and skills are often needed to break conventional ways of looking at problems. Diversity can take a wide variety of dimensions: gender, age, educational background, ethnicity, discipline, and so on. When selecting teams this should be taken into account. A team of pure software engineers, consisting of middle aged white European males, is less likely to devise a rounded solution, or even an innovative one, than a more diverse team. Diversity should be encouraged and become a normal and praised feature of innovation teams, including those that deal with incubation.

4.2 Coordination and Management

4.2.1 Establishment of the Programme Board

In order to ensure proper internal coordination and effective prioritization of NATO needs, it is recommended that an innovation programme board is established, involving all relevant stakeholders from NATO. The prime purpose for the programme board is to drive the programme forward and deliver the outcomes and benefits. Members will provide resource and specific commitments to support the Senior Responsible Owner who is accountable for the successful delivery of the programme.

4.2.2 Efficient Process to Enable Incubator Activities

Conventional processes and regulations governing sharing of information or payments from NATO were not well suited to the short-term, low-cost, agile nature of the incubator.

The development of a standard legal agreement describing information sharing, non-disclosure, IPR and payments would simplify and speed up the administrative effort needed to support incubator activities. This could replace the custom-made agreements which are currently in use, each based on the external partner's usual non-disclosure agreement.

While the *grant* collaboration mechanism results in NATO funds being paid to industry or academia, the intent is very different in comparison to the conventional NATO acquisition process. A simpler mechanism that treats incubator grants differently to acquisitions would simplify the process for both NATO and the incubator partners.

4.2.3 Well-defined Project Initiation Process

The process of identifying needs, prioritizing them, harvesting innovative ideas and making final project selections is essential in order to ensure the effective exploitation of the developed solutions through the NATO common funded procurement process or other methods. Thus, it is recommended that a well-defined and agreed process is followed during the innovation project initiation phase, ensuring proper involvement of all stakeholders and proper funding of the activities.

Identifying needs and harvesting innovative ideas should draw on all sources available across NATO and Nations, and should include specialists in identification of threats and technology subject matter experts, as well as IT service providers and the user community. The relevant stakeholders within NATO include the Cyber Defence Committee (CDC),[20] Emerging Security Challenges Division (ESCD),[21] the Collaborative Cyber Defence Centre of Excellence (CCD CoE),[22] the Science and Technology Organization (STO),[23] Allied Command Transformation (ACT),[24] Allied Command Operations (ACO),[25] and the NCI Agency.[26]

An important open question is whether this large group of the stakeholders in NATO cybersecurity can provide the required support to the innovation activities as part of their regular activities, or whether an additional mechanism or organization is needed. Prioritization of the identified needs, to make final project selections, is a process which should be inclusive of all interested parties, while being as responsive as possible.

4.2.4 Timescale

Sufficient time shall be planned for both project initiation and project execution. It is recommended that the initiation phase (from identification of the innovation needs and ideas to project selection) takes 3 to 6 months, and the project execution phase takes 6 to 12 months. These longer timescales would be particularly beneficial to smaller companies and would encourage their involvement within the NATO Cyber incubator.

Many industry and academic partners indicated that it is difficult, if not impossible, to assign resources to otherwise interesting activities at such short notice. Advanced planning and advertising of the intent to use this methodology can help.

4.2.5 Resources

The pilot project showed that running an incubator requires a high level of involvement from the NCI Agency staff, in order to drive the collaboration projects in the right direction and deliver benefits. As a consequence, the appropriate resourcing of innovation projects with NATO subject matter experts should be considered as a key element for the success of the initiative.

Execution of innovation projects is a resource intensive activity and a proper staffing of the innovation activities needs to be ensured. Sufficient availability of internal personnel not only increases the chances of the project success, but also increase the capability for transferring project results to the NATO capability development and procurement processes.

It is difficult to request funding on the same timescale as needed for project initiation. Seeking funding only after projects are identified will not allow the reaction times needed. Therefore, it is recommended that an overall core funding source (or budget) be established for these activities. Specific technical activities would be selected and then funded within this overall budget. Additional contributions could be made by any parties, e.g. NATO, Nations, industry, but that would be in addition to the core funding.

4.3 Communication and Collaboration

4.3.1 Communication Platform

The build-up and maintenance of the innovation ecosystem is a critical and resource intensive activity. Care should be taken that enough human resources and time are reserved for these tasks. An effort shall be made to provide direct and open communication with potential partners, including the initial stages of the initiative design. Responses received during the pilot project suggested that industry appreciated this and it made NATO seem much more open and accessible.

It is recommended to develop a common strategy for addressing partners' interests regarding procurement and capability development issues in relation to the innovation activities. This would ensure that all possible questions can be answered swiftly and correctly, and guarantee that the discussion about wider perspective does not obscure the main objectives of the specialized technical events.

4.3.2 National Platforms and Clusters

Establishing direct contact with the widespread cybersecurity industry would require resources which are unlikely to be affordable to NATO. Therefore, an integrated plan for involving and leveraging existing national cybersecurity platforms and clusters within NATO and partner nations should be developed and maintained.

The national cybersecurity platforms and clusters offer several important advantages for NATO innovation activities. First of all, they enable reduction of the coordination and travel costs by offering access to lots of companies at the same time. They also isolate NATO from direct interaction with specific companies, thus proper care has to be taken that direct communication channels with industry and academic partners are maintained and only facilitated and amplified through the involvement of national cybersecurity platforms and clusters.

Although, inherently, the national clusters are focused on supporting national industry, it was experienced that clusters are interested in information sharing and involvement of foreign partners, mainly with the objective of attracting them to help foster their local economy. This natural interaction can be exploited by NATO to help synchronize cybersecurity activities between different nations. The current experience has shown that there has not been an unacceptable bias when working with a specific national cybersecurity collaboration platform, e.g. HSD.

4.3.3 SME Collaboration Partners

Although potentially of higher risk, there are considerable benefits in working with SMEs and start-ups in the development of innovative cyber defence solutions. Further effort should be made in the future to *take the risk* and select SMEs to partner with, harness their innovative potential and help mitigate the lack of adequate investment and visibility they often face. Smaller companies are more dynamic and able to provide product development to accommodate our requirements while offering agility, flexibility, innovation, commitment, customer focus, and niche or specialist kills and capabilities. To take full advantage of partnerships with SMEs, a pilot project targeting exclusively SMEs should also be considered, as having to compete with large companies often discourages SMEs from participating.

4.3.4 Collaboration through ACT

The ACT Innovation Hub provides a natural reach out opportunity towards North American innovation partners. The cybersecurity innovation incubator can also leverage collaboration infrastructure and processes already established by the ACT Innovation Hub in order to reach out efficiently to a larger set of stakeholders.

4.3.5 Collaboration through STO

Collaboration with STO can include several dimensions. First of all, results of STO activities, including working groups, exploratory teams, seminars, van Karman horizon scanning, etc. provide valuable input for defining the prospect focus area for innovation activities. Secondly, STO can be used as an outreach towards national research organizations, industry and academia in order to provide proper awareness about, and participation in, NATO innovation programmes. Furthermore, STO activities can be used as a dissemination and additional discussion channel for the results of the innovation projects.

4.3.6 Collaboration through CCD CoE

The primary role of the CCD CoE is to provide an environment for gathering and developing cybersecurity requirement from its Sponsoring Nations. Through the Requests for Support received from its Sponsoring Nations, the CCD CoE has a good overview of the innovation needs of its stakeholders. These requirements could influence the focus areas chosen for the innovation projects.

CCD CoE could also participate in the Innovation Programme Board and provide subject matter experts for the evaluation of the project proposals. Moreover, CCD CoE could act as an additional outreach partner towards industry and academia within participating NATO nations. The CCD CoE events, including both cyber exercises (e.g. Locked Shields) and conferences (e.g. CyCon), could be used as an effective dissemination channel and validation environment for the results of the innovation activities.

Finally, the opportunities for direct involvement of the CCD CoE subject matter experts into the execution and support of the individual innovation projects is a matter that that should be further discussed between the CCD CoE and its sponsoring Nations.

4.4 Infrastructure

4.4.1 Collaboration Infrastructure

An effective collaborative IT environment offers several important advantages. In addition to enabling information sharing, it also allows a community to interact freely on a wide range of innovation topics.

During the incubator execution, the collaboration environment provided by the Distributed Networked Battle Labs (DNBL) framework [27] was used. The DNBL provides a web based environment for communities of interest (COIs) to facilitate linkage and coherency between national and NATO capability interoperability development efforts. It is based on the concept of collaboration between different COIs through built-in document sharing features. These document-sharing features were very relevant to the information sharing needs of the cyber incubator, but they turned out to be insufficient for fostering effective collaboration. The additional required features included remote presence and a conferencing environment, versioning capabilities beyond Microsoft documents, and a scientific and technical citation system.

A number of existing collaborative IT environments are currently being assessed for their suitability to the future needs of NATO and its incubator partners. The final selection of the collaboration environment will be performed based on offered functionality and cost.

4.4.2 Integration Infrastructure

Cyber defence capability development in NATO would benefit from the availability of an integration platform that would allow innovation stakeholders to develop, share and enhance an interoperable collection of CIS security solutions and systems. In their technical report,[28] the STO IST-096 research task group provides an initial specification of an integration platform that could be used by NATO and NATO Nations to address this problem.

The benefits of providing a common platform for research and development are the following:

- Foster technology advancement in CIS security;
- Enable independent and interoperable research and development;
- Enable rapid exploitation of innovations from (and to) industry, academia, and allies;
- Align research and development on a common framework.

Without an integration platform, each innovative solution stands alone, and does not leverage and build upon the other current and new solutions. Further, operators require specific training for each, which wastes time and resources. Any integration

platform must support not only cybersecurity, but also the core and functional IT services which cybersecurity functions protect.

It is recommended that an integration platform, representative of a NATO CIS and able to support cybersecurity innovations, is adopted and made available to solution providers in both independent (e.g. virtual machines) and hosted (e.g. on the NATO cyber range) configurations. Solution providers could then install and demonstrate their solutions in a simulated NATO context. Beyond providing the environment, it is recommended that solution providers be required to demonstrate their solutions on the integration platform so that all solutions are compared under the same conditions, and so that all innovations, though built independently, can fully leverage the other solutions on the integration platform.

4.4.3 Proposal Handling Infrastructure

In order to increase efficiency, compliance with requirements, and accountability, an electronic system should be implemented supporting submission, handling and evaluation of proposals. Such a system could be based on, or used for, submission of innovation proposals across a range of technology areas.

4.5 Legal Considerations

4.5.1 Delineation with NSIP Procurement

Tasks and activities associated with this programme of collaborative innovation projects need to be carefully coordinated with the appropriate NATO bodies in the event any acquisition activity is anticipated and/or authorized under the NATO Security Investment Programme (NSIP)[29] or other funding arrangements. This is to ensure that there is no unfair advantage for prospective bidders, or conflict of interests with any project or programme. Exclusion clauses, where considered appropriate, may be applied on a case by case basis but any exclusion will be considered exceptionally.

4.5.2 Release of Calls for Participation

The NCI Agency, based upon the initial focus areas and selected business cases, is responsible for the invitation to candidates based upon the level of interest from industry and the NATO (and partner) nations. Future collaborative innovation projects will be announced by a call for proposals, followed by a kick-off event or formal documented invitation and followed by a workshop where industry, government and academia can present their cases under stated evaluation criteria.

Invitations will be issued to those nominated/selected companies, academia or government organizations in accordance with NATO acquisition policy and procedures. Industry, government and academia are encouraged to enter into arrangements with NATO, such as the Basic Ordering Agreements (BOA),[30] a recognized NATO pro-

gramme with policy and procedures, so that NATO has a ready repository of expertise, skills and experience in addition to agreements, and terms and conditions, that can be readily used once candidates have been selected. The BOA programme may not be appropriate for all organizations such as government and academia but similar arrangements can be established through Memoranda of Agreement or Technical Arrangements, depending on the requirement.

4.5.3 Selection of Candidates

The Innovation Programme Board under the jurisdiction of the appropriate committee will be responsible for the selection of candidates based upon the selected focus areas and business cases and proposals provided by the appropriate NATO committees and bodies.

Proposal evaluation and recommendations will be made by the subject matter experts responsible for the individual focus areas who evaluate the proposals (in conjunction with NCI Agency involvement) and make recommendations for those proposals to take forward, based on key criteria including operational relevance, technical relevance, costs and risks.

Following evaluation, recommendations will be made to the Innovation Programme Board for final selection of the candidates commensurate with the funding arrangements available for the specific round of *call for proposals*.

Subject to the final selection of candidates, both successful and unsuccessful candidates will be notified. Contracts will be established with the selected candidates in accordance with the appropriate acquisition and financial procedures.

As a result of the analysis of the pilot innovation programme, we have identified that we should be looking at several factors in the selection:

1. The technical merit of the proposed solution to the problem. This should consider the match of the solution to the problem and the technical merit of the solution;
2. The likelihood that the solution can be delivered in the defined time frame. This needs to consider the maturity of the solution proposed and the timeframe within which the solution is needed;
3. The team being proposed. This needs to evaluate if the company is willing and able to bring the commitment, agility and speed needed to make the idea a success;
4. The through life costs. An initial understanding of the through life costs of the solution should it be put into production, needs to be considered.

Much of the selection is going to be down to the judgment of subject matter experts, and, consequently, will be less rigorous than a formal government competition usually allows.

4.5.4 Terms and Conditions for Intellectual Property Rights

In line with the principles, aims and objectives captured above, intellectual property rights (IPR) will be applied on a mutually beneficial basis. Generally, NATO will apply terms and conditions which are mutually beneficial to Industry and NATO, and to permit NATO to use data, disseminate information and take copyright in the work to be performed. The rights applied shall be sufficient to enable NATO to use the results of any specific innovation work performed by the candidates for the relevant business.

4.5.5 Legal and Contracting Framework

Generally, the processes above will be conducted in accordance with the NATO acquisition policy, procedures and regulations subject to the funding source, direction and the authorizations of the appropriate committees, budget holders and programme boards responsible. Tasks and activities contracted under this selection will be subject to a contractual arrangement, whether this be a contract with industry or an agreement with government or academia, which requires a mutually agreed arrangement between the parties.

5 Transition from Incubation to Operation

While the approach used in the incubator pilot activity proved useful to identify, understand and begin to mature promising technologies of potential value to NATO, an open issue remains as to how best to pull these ideas through into service operations in timeframes that are relevant to the expressed needs.

Normally, acquisition of NATO operational capabilities (on which end-user services are based) are the subject of the NATO Security Investment Programme (NSIP). This framework, while providing good visibility and governance, can consume many years from inception to capability delivery, as it involves a number of lengthy stages − Capability Package (CP), Joint Staff Screening Report (JSSR), Type B Cost Estimates (TBCE), Invitation for Bids (IFB), Contract, delivery of the capability by industry and ultimately transition into service operations. There are abbreviated processes for urgent requirements but even when approved for use these can take considerable time to deliver capability.

Whereas many decades ago defence requirements spearheaded the development of new technologies (such as the Internet), and in that way drove progress in the commercial world, today the situation is reversed and keeping with the advancements that

are being fielded in the commercial world is a challenge for NATO and most NATO Nations. The NATO processes have now reached the point where they are lengthier than the expected life of the IT capabilities that are being acquired. This means that the next cycle of the process has to begin before the previous has even begun to deliver. This increases the risk of projects delivering yesterday's technology that is no longer relevant.

Our potential adversaries are likely to be less constrained by lengthy acquisition processes and so they can quickly adopt the latest commercial offerings to meet their needs. This is true across the whole of the IT domain but perhaps most germane in the area of cyber defence. NATO must find ways to balance the internal checks that the NSIP processes provides with the compressed timelines that it must be responsive to if it is to stay relevant. If after completing an incubation activity nothing is put into service for several years, then it will in many cases be of little relevance before it arrives.

In the incubation activity that was undertaken, there was no the scope to define a solution to this problem; rather it was identified that there is need to develop a path that can take capability from an incubator environment and transition it to service operation in a relevant timeframe. An initial set of principles for such a process were identified:

1. Agility is key. Change is the norm and the process needs to be able to deal with continual change of both requirements and solution possibilities;
2. Governance needs to be based on outcomes, not on processes. The current model allows checks and balances to be made at every stage of the path leading to lengthy implementation cycles. The trend is towards ever increasing checks, and additional governance. More attention needs to be put on the ends rather than the means;
3. Development of IT systems is moving from a paradigm of time-boxed projects delivering fixed capability to a *continuous development* paradigm. Major projects need only be undertaken when there is a step change in capability needed. The norm is for changes to be small, continuous and relevant. This is true across software development, infrastructure enhancements and cyber defence evolution;
4. Start / stop funding cannot keep up with the pace of change in the threat and the solutions spaces. The norm needs to be a constant stream of resources that are available to evolve capability to match the continuously changing need; and
5. Competition needs to occur early in the process, likely at incubation, before requirements are fully defined and before solutions are developed, matured

and understood. This allows the development of the solution without prejudicing future competitions in favour or against the organizations involved in the incubation. It favours innovation and industries of all sizes rather than favouring large industry alone.

These principles should be further developed and refined in future cyber incubator activities.

Possible Competition and Exploitation Models

Several models are open to ensure that competition takes place within the incubator deployment process. The conventional NATO procurement methods are based on an environment where the requirement, threat and technology do not move rapidly. Figure 1 shows how current procurement projects can factor in the acquisition time in order to deliver current technological solutions.

This mechanism may be effective where there is a long and stable history of technological development. Cybersecurity is one area where there is less stability or predictable trends in technology development and therefore the model of Figure 2 may not align well with the rate of technological change, either to the solutions or to the threats / requirements.

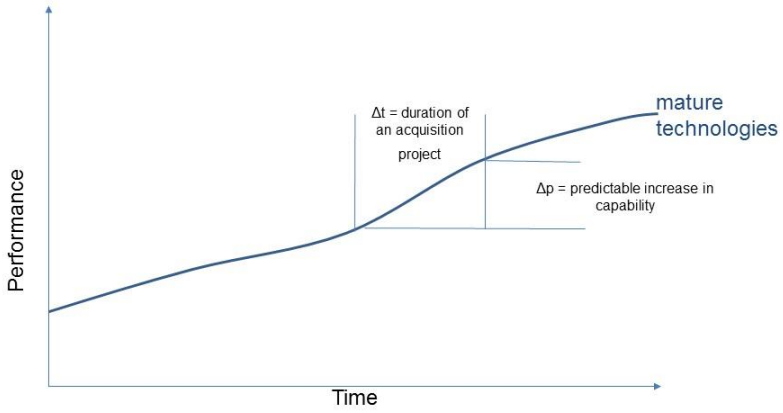

Figure 1: Mature technology performance and procurement process.

The incubator concept was conceived to de-risk and dramatically decrease the time to develop responses to the NATO cybersecurity challenges. It provides a more responsive model for cooperation between NATO and suppliers (industry, academia) in sharing challenges and potential solutions. There are a number of models for NATO to apply solutions developed through a cybersecurity incubator. The level of effort for enterprise-wide deployment of incubator outputs may be significant. Below are some possible options to balance the competitive nature of NATO procurement processes with the agility needed to adequately support the NATO cybersecurity posture.

Option 1: Competition at incubator proposal stage: The calls for incubator proposals shall be openly distributed. The process to select and resource proposals shall be clearly documented. Estimated costs to deploy the results of the incubator output shall be included in the proposal and shall be considered during selection of proposals. NCIA will have the option to carry out an enterprise wide deployment of incubator proposals in conjunction with the proposing organization.

Option 2: Competition at incubator completion stage: Proposals will be screened and an impartial assessment made of which incubator proposals to support. Proposals which are supported and which lead to outputs which NATO wishes to deploy enterprise-wide will then be used as input to a competitive process. Enterprise-wide de-

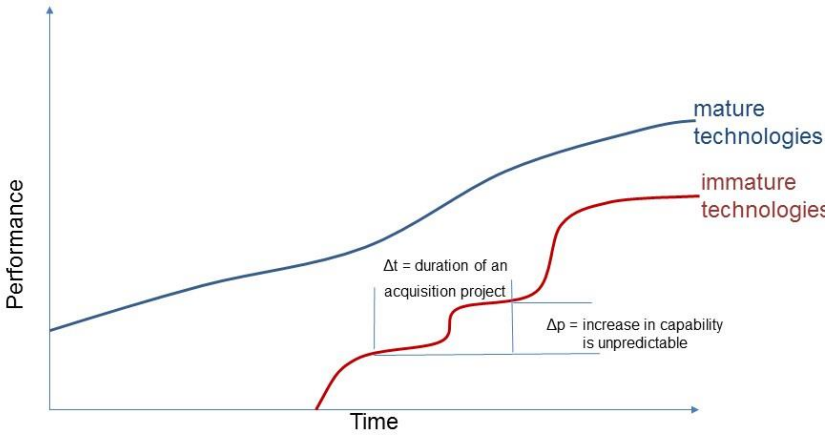

Figure 2: Immature technology performance and procurement process.

ployment will be treated as a separate procurement, conducted in accordance with NATO acquisition regulations. It is recommended that the default position is that the incubator proposer is allowed to compete in this process.

Option 3: Competition of enterprise-wide deployment: A priory, NATO conducts a competition to identify a partner which could conduct the enterprise-wide deployment of successful incubator outputs. This would use a similar mechanism to that used at present to compete the service support contracts, where the exact scope and scale of a task is not known. This has the advantage that deployment is not delayed by the need for competition after the incubators complete.

Option 4: Incubator partner deploys: In this option the successful incubator partner is given the option to conduct the enterprise-wide deployment at a cost to be defined by NATO (based on NCIA expertise in cost-estimation). This procurement model would require changes to the current procurement regulations, but speeds up the option for deployment.

6 Conclusions

The ever-increasing pace of technological development, as well as emergence of new stateless adversaries and threat vectors, makes the traditional NATO approach to the technical capability development inadequate for addressing the emerging security challenges in cyber space. In order to mitigate this situation, we describe an incubator framework, which provides a physical and virtual environment enabling industry, in particular small and medium-sized enterprises, science and technology organizations, academia, and national defence labs, to collaborate on innovation projects on the basis of either voluntary, nationally funded or NATO commonly funded contributions.

The proposed incubator framework has been practically validated and technical results have confirmed the feasibility as well as the benefits of setting up a cyber incubator within NATO. This disruptive approach to capability development has demonstrated effectiveness in approaching technical challenges in a rapidly moving field, through close and agile work between diverse partners.

The main lessons learned from our experiment result in a number of recommendations, including required changes to the internal and external NATO processes and procedures and the adoption of a new innovation-friendly and risk-tolerant organizational culture within NATO.

Key recommendations include the leveraging of existing communication and laboratory infrastructure as well as the expertise and processes developed by the NCI Agency, industry and ACT in support of innovation. An integration platform would

provide innovation stakeholders with an environment representative of NATO CIS in which specific products or solutions can be developed and demonstrated with the objectives of enabling independent and interoperable solution development, as well as rapid intake of emerging cybersecurity technologies to respond to global threats.

It is also necessary to consider the funding model. Funding should be made available to provide external stakeholders with a financial incentive to address NATO specific technical challenges in a predictive manner. This should help facilitate cooperation though the incubator and will broaden the range of participants.

Whilst the incubator has successfully demonstrated the ability to provide a framework to bring rapid results from academia and industry to NATO, it needs to be extended to facilitate the outputs being deployed by NATO for operational use. This could be the target of a second stage of the incubator.

References

1 Nicklaus A. Giacobe, "Application of the JDL Data Fusion Process Model for Cyber Security," *Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications*, volume 7710 (SPIE, 2010), https://doi.org/10.1117/12.850275.

2 Yan Zhang, Shuguang Huang, Shize Guo, and Junmao Zhu, "Multi-sensor Data Fusion for Cyber Security Situation Awareness," *Procedia Environmental Sciences* 10, Part B (2011): 1029-1034, https://doi.org/10.1016/j.proenv.2011.09.165.

3 Yogesh L. Simmhan, Beth Plale, and Dennis Gannon, "A Survey of Data Provenance in e-Science." ACM SIGMOD Record 34, no. 3 (September 2005): 31–36, https://doi.org/10.1145/1084805.1084812.

4 Luc Beaudoin, Michael Froh, Marc Gregoire, and Julie Lefebvre, "Computer Network Defence Situational Awareness: Information Requirements," in *Military Communications Conference*, 23-25 October 2006, https://doi.org/10.1109/MILCOM.2006.302231.

5 Philippe Lagadec, L. Dandurand, E. Bouillon, Konrad Wrona, S. Torrente, "Cyber Defence Situational Awareness and Dynamic Risk Assessment," Presentation at the *NATO Research and Technology Organisation Symposium on Information Assurance and Cyber Defence*, IST-091 (Tallin, Estonia, 2010).

6 Michael Stonebraker, "SQL Databases v. NoSQL Databases." *Communications of the ACM* 53, no. 4 (2010): 10–11, https://doi.org/10.1145/1721654.1721659.

7 https://www.elastic.co/.

8 Philippe Lagadec, "Visualisation et Analyse de Risque Dynamique pour la Cyber-Défense," in *Symposium sur la Sécurité des Technologies de l'Information et de la Communication* (SSTIC), Rennes, 9-11 June 2010, pp. 3–31, https://www.sstic.org/2010/presentation/CyberDefense/.

9 Lagadec, Dandurand, Bouillon, Wrona, and Torrente, "Cyber Defence Situational Awareness and Dynamic Risk Assessment."

[10] Alessandro Armando, Gabriele Costa, and Alessio Merlo, "Bring Your Own Device, Securely," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, SAC'13, Coimbra, Portugal, 18-22 March 2013, pp. 1852–1858, https://doi.org/10.1145/2480362.2480707.

[11] Alessandro Armando, Gabriele Costa, Alessio Merlo, and Luca Verderame, "Enabling BYOD Through Secure Meta-market," in *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*, WiSec'14, Oxford, United Kingdom, 23-25 July 2014, https://doi.org/10.1145/2627393.2627410.

[12] A more detailed discussion of project results can be found in Alessandro Armando, Gabriele Costa, Alessio Merlo, Luca Verderame, and Konrad Wrona, "Developing a NATO BYOD Security Policy," in *Proceedings of the International Conference on Military Communications and Information System*, ICMCIS, Brussels, Belgium, 23-24 May 2016, https://doi.org/10.1109/ICMCIS.2016.7496587.

[13] Attaullah Buriro, Bruno Crispo, Filippo Del Frari, Jeffrey Klardie, and Konrad Wrona, "ITSME: Multi-modal and Unobtrusive Behavioural User Authentication for Smartphones," in *Technology and Practice of Passwords*, ed. Frank Stajano, Stig F. Mjølsnes, Graeme Jenkinson, and Per Thorsheim, Lecture Notes in Computer Science, vol. 9551 (Springer, Cham, 2015), 45–61, https://doi.org/10.1007/978-3-319-29938-9_4.

[14] Attaullah Buriro, Bruno Crispo, Filippo Frari, and Konrad Wrona, "Touchstroke: Smartphone User Authentication Based on Touch-Typing Biometrics." in *New Trends in Image Analysis and Processing − ICIAP 2015 Workshops*, ed. Vittorio Murino, Enrico Puppo, Diego Sona, Marco Cristani, and Carlo Sansone (Springer, Cham, 2015), 27–34, https://doi.org/10.1007/978-3-319-23222-5_4.

[15] Attaullah Buriro, Bruno Crispo, Filippo Delfrari, and Konrad Wrona, "Hold & Sign: A Novel Behavioral Biometrics for Smartphone User Authentication," in *Proceedings of the Mobile Security Technologies Workshop* (MOST), in conjunction with 37th IEEE Symposium on Security and Privacy, San Jose, CA, 26 May 2016, http://www.ieee-security.org/TC/SPW2016/MoST/.

[16] Agnes Desolneux, Lionel Moisan, and Jean-Michel Morel, "The Helmholtz Principle," in *From Gestalt Theory to Image Analysis*, Interdisciplinary Applied Mathematics, vol. 34 (Springer, 2008), pp. 31–45, https://doi.org/10.1007/978-0-387-74378-3.

[17] Alexander Balinsky, Helen Balinsky, and Steven Simske, *On the Helmholtz Principle for Data Mining*, Technical report HPL-2010-133 (HP Laboratories, 2010), www.hpl.hp.com/techreports/2010/HPL-2010-133.pdf.

[18] Alexander Balinsky, Helen Balinsky, and Steven Simske, "Rapid Change Detection and Text Mining," in *Proceedings of the 2nd IMA Conference on Mathematics in Defence*, Defence Academy of the United Kingdom, Swindon, UK, 20 October 2011, pp. 1–6.

[19] Konrad Wrona, Sander Oudkerk, Alessandro Armando, Silvio Ranise, and Lisa Ferrari, "Assisted Content-based Labelling and Classification of Documents," In Proceedings of the International Conference on Military Communications and Information System (ICMCIS), 23-24 May 2016, https://doi.org/10.1109/ICMCIS.2016.7496589.

[20] http://www.nato.int/cps/en/natohq/topics_78170.htm

[21] https://esc.hq.nato.int/

[22] https://ccdcoe.org/

[23] https://www.cso.nato.int/

[24] http://www.act.nato.int/

[25] http://www.aco.nato.int/

[26] https://www.ncia.nato.int/

[27] https://dnbl.ncia.nato.int/

[28] James Sidoran, *Information Assurance / Cyber Defence Research Framework*, Technical Report STO-TR-IST-096 (Paris: NATO Science and Technology Organization, 2014), https://doi.org/10.14339/STO-TR-IST-096.

[29] http://www.act.nato.int/nsip

[30] https://www.ncia.nato.int/Industry/pages/basic-ordering-agreements-boa.aspx

About the Authors

The team of authors is with the NATO Communications and Information Agency, https://www.ncia.nato.int/, at the premises located in The Hague, The Netherlands.