CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Recent Cyber Events and Possible Implications for Armed Forces

A look at the trends from 2020 and towards the future

#8 – January 2021

About this paper

This paper is the collaborative view of NATO CCDCOE researchers highlighting the potential effects on the military of current events and of developments in cyberspace during 2020, based on publicly available information. It does not set out to be exhaustive. While the authors have made every effort to describe events from a perspective relevant to NATO and partner nations, there may be national and regional differences which this paper does not address.

The authors of this paper are independent researchers at the NATO CCDCOE; they do not represent NATO, nor does this paper reflect NATO's position. The aim of the paper is not to replace information about vulnerabilities and incidents provided by CSIRTs and providers of CIS products and services.

1. 2020 ends with a massive supply chain attack

In December 2020, several US government agencies were breached by a software supply-chain attack. The operation, which was initially launched as early as March 2020, clearly shows how a breach of a trusted supply chain can affect a large number of targets and how an advanced adversary can operate undetected for a long time.

> 'The US has suffered a massive cyber breach. It is hard to overstate how bad it is.' (Bruce Schneier in *The Guardian*)

The full scope of the breach is still unfolding but it is clear that a backdoor dubbed SUNBURST had been installed in thousands of networks. Research from FireEye and Microsoft indicate that about 50 organisations had been targeted and seriously affected, including Microsoft and several US government agencies. The number of targets may number more than 250 organisations. The number severely affected still remains low, relative to the large number of infections, but this is most likely the result of the actor behind the attack picking the targets to attack further. A joint statement released on 5 January states that 'fewer than 10' US government agencies were compromised. The extent and method of the attack should be a cause for concern for military organisations given military dependence on civilian institutions for the operations and maintenance of their ITC infrastructure.

In some ways, the attack is reminiscent of the NotPetya attack in 2017 which used updates for a software package commonly used in Ukraine as the vehicle to get malware into the target systems. In the current case, the vehicle was the update chain of network management software SolarWinds Orion. The objective seems to have been espionage rather than to disrupt operations, although the backdoor may provide a future opportunity to exploit the vulnerability.

Several sophisticated techniques both to evade detection and to move laterally in compromised networks have been found. This also allowed the adversary to maintain a persistent presence in the networks. This indicates that an advanced, probably state-backed actor is behind the compromise. This sophisticated attack is widely thought to be tied to Russia with the group APT29, also known as 'Cozy Bear', being named in some reports. Russia has denied responsibility for the attacks.

The security of the supplier's software update mechanisms seems to have been lacking. Reports suggest a weak password may have allowed access to the update servers. Better mechanisms to assess the security of the software supply chain are clearly needed. It is not feasible for every customer of a supplier to

independently audit the security measures put in place; this calls for interagency and international cooperation in realising some type of independent assessment and certification of software used in critical industries and the government.

Microsoft also reported that source code in their network had been accessed as part of the breach, but no code was modified. Undetected manipulation of, for example, Windows or Microsoft Office source code would of course have provided an opportunity for an even wider supply chain attack, but there is no evidence of that. That the attackers were able to view Microsoft source code, while not good, does not have to be a major security concern. Software should never be designed so that its security relies on keeping the code secret. Access to the code may, however, aid an attacker in understanding the software and identifying previously unknown vulnerabilities.

The knowledge of the attack we now have affords many opportunities to detect and remove backdoors but the challenge is to ensure that the attacker does not maintain a foothold in parts of a network when the initial backdoor is removed and that cyber defenders can detect similar attacks. The attacker has likely tried to compromise other parts of the network after getting initial access, making cleaning the network more problematic. An even more difficult situation is if there is suspicion that data in the network may have been manipulated and can no longer be trusted. A thorough investigation of all parts of the compromised network is needed, including audits of logs and integrity checks of installed software and data. This may require outside help if the organisation does not have sufficient competence or resources.

Both the relative ease with which the initial malware was able to beacon and connect to command-and-control servers undetected and the way the attackers could then move around the compromised networks highlights the need for a strategy of defence in depth. Strict restrictions on how even trusted equipment is allowed to communicate inside the enterprise network and with internet are needed to make these operations more difficult to execute. Insecure application programming interfaces (APIs), too much trust in network equipment and reuse of credentials for machine-to-machine communication are examples of vulnerabilities that can be used by an attacker when moving laterally in the network. More advanced detection systems such as using machine learning techniques in detecting anomalies may help prevent breaches like this going undetected for so long.

2. Developments in international law and cyber norms during 2020

While the COVID-19 pandemic has understandably obscured many other important events of 2020, it has also brought new food for thought to those working on how international law applies to cyberspace in peacetime and in armed conflict.

In the first place, the pandemic has shown the vulnerability of the healthcare sector and of those who depend on it. Cyber operations against hospitals including those responsible for COVID-19 testing (for example in France, Spain, Thailand, the United States or the Czech Republic), cyber espionage activities attributed to state actors in respect of vaccine research facilities and spreading disinformation and fake news online (including by governments) have been unprecedented.

The developments have prompted several reactions by the international law community. In the same spirit as the July 2020 ICRC proposal for adoption of a norm specifically protecting medical facilities from cyberattacks, renowned international law experts have called for better protection in the Oxford statements on international law protections against cyber operations targeting the healthcare sector and on safeguarding vaccine research. Universal condemnation by states of this wave of malicious cyber operations against the healthcare sector puts into perspective the refusal by some states to acknowledge the application of international humanitarian law (IHL) to cyberspace. If it is unlawful to target hospitals with cyberattacks including during an armed conflict, under what body of law if not IHL?

While IHL rules' applicability to cyber may not yet be accepted by all, the number of states explicitly recognising it has grown in 2020. In December 2020, Israel published its national position on international law following pronouncements by Finland, New Zealand, and the Czech Republic. The Strategy and Governance section of CCDCOE's digital library offers a collection of primary sources including statements on international law.

States' positions on international law are continuously incorporated into and operationalised in the scenarios of the Cyber Law Toolkit and reflected in the Centre's country reports series which has been complemented by thematic webinars in 2020, beginning with Italy.

With NATO recognising space as an operational domain in December 2019, continued attention also needs to be given to cybersecurity aspects of space operations, as highlighted by researchers including those from CCDCOE. Evolving technologies have been among the Centre's long-term interests. A new book on autonomous capabilities seen from a multidisciplinary perspective will enrich the existing research on autonomous capabilities and cyber means and methods of warfare in 2021.

With the growing incidence of malicious cyber activities in cyberspace, the willingness of states to denounce the attackers also increases. 2020 saw the first practical application of the 2017 EU Cyber Diplomacy Toolbox and targeted cyber sanctions. We can expect more to come in the future, considering the recurring attacks on important governmental institutions in Europe (e. g. Norway or Estonia).

> 'Most noteworthy was that there seems to be an increasing readiness amongst states to come forward with their positions on international law' (Overview of the UN OEWG developments: continuation of discussions on how international law applies in cyberspace)

All these developments have been taking place against the backdrop of ongoing UN-sponsored processes on norms of responsible behaviour in cyberspace, the UN Governmental Group of Experts and the Open-Ended Working Group. Although the latter has had to postpone the presentation of its conclusions to the Secretary General due to the COVID-19 pandemic, there have nonetheless been lively discussions on the application of international law in cyberspace.

This shows that analogies of cyber to the Wild West or references to wars fought without international norms are misplaced. While a certain level of norms-scepticism may be understandable, the developments in 2020 only confirm that international law is ever more relevant to help nations and their militaries face new challenges. Amongst others, universally accepted norms of state behaviour in cyberspace and the certainty that comes with them are likely to provide greater deterrence to malicious state actions and offer additional tools to bring offenders to accountability. The time is ripe for Tallinn Manual 3.0, a project that will revise and expand the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. The updates will address the evolving nature of cyber operations and state responses, and add new topics of importance such as official statements on international law and the UN-level discussions on responsible state behaviour in cyberspace.

3. Supply chain risks a major concern for governments as 5G infrastructure is rolled out

The debate regarding 5G escalated in early 2019 along with growing concerns about the security of both commercial and military communications within national and Alliance networks. The conversation primarily focused on the risks posed by Huawei and other Chinese suppliers of 5G network technology. The importance of secure communications, including 5G, was stressed by NATO leaders at the meeting in London in December 2019. The meeting highlighted the need 'to rely on secure and resilient systems' to ensure national security as military communications begin to transition to 5G.

However, military operations do not take place in a vacuum; they are, to a large extent, reliant on civilian infrastructure to function. The boundaries between civilian and military use of the internet and telecommunications networks, including 5G, are difficult to determine. The roll-out of 5G networks will increase both communication speed and with a plethora of new possibilities such as wider adoption of the internet of things (IoT), a network of devices which depend on internet connectivity to function. With many interconnected IoT devices from self-driving cars to smart electrical grids and from remote surgery to consumer devices, we will begin to understand the security of IoT and our networks, as well as end-user devices, is becoming increasingly important.

> 'It is rational to demand the highest possible security assurance from 5G technology used for critical communication.' (Huawei, 5G and China as a Security Threat)

The choice of supplier of 5G network technology is a national matter which traditionally has been made by telecommunications operators. These choices have consequences for both NATO and the EU. Both organisations have added 5G security considerations to their risk assessments and mitigation measures. However, stakeholders including national governments, telecommunications service providers, technology suppliers and government, business and individual end users have different risk perceptions and appetites. The underlining principle for legislators, operators and suppliers must be to provide customers a 'secure by design' network.

Based on the EU coordinated risk assessment of 5G networks security, the EU Toolbox for 5G security has laid out a range of security measures. These initiatives provide methodologies for risk mitigation to ensure secure 5G networks are deployed across Europe. For each of the identified risks the toolbox sets out comprehensive plans for mitigation and recommends a set of both key strategic and technical measures to be taken by member states and the Commission. The strategic measures include regulatory powers, third party suppliers, diversification of suppliers and sustainability and diversity of the 5G supply and value chain. The technical measures include baseline and 5G-specific measures for network security, requirements related to suppliers' processes and equipment and resilience and continuity.

The CCDCOE's report on Huawei, 5G and China as a security threat describes the legal and political environment in China and the possible security implications. As Chinese companies are under a legal obligation to cooperate with domestic intelligence services, more and more countries in North-America, Europe and the Asia-Pacific region have either phased out, limited or, in some cases, excluded these companies. The most notable 5G technology supplier is Huawei, which has experienced delays in the roll-out of its 5G technology. Supported by the Chinese government, Huawei provides telecommunications networks and infrastructure in many emerging markets as part of China's Belt and Road Initiative (BRI).[1] With a keen eye for long term strategy, the Chinese will continue to compete to dominate the market for future technologies such as 6G.

Today many European countries are in the process of updating their telecommunications legislation and enforcing new regulations in accordance with the recommendations of the EU 5G Toolbox and with EU and WTO trade rules. The EU regulations are not specifically directed against China or any other country or supplier, but will be a necessary legislative follow-up to the technological developments.

As companies like Ericsson and Nokia have to adhere to EU rules regarding state aid, they may not be able to compete on price with Chinese companies. With the close of 2020 it seems that countries have increasingly realised the importance of secure and resilient telecommunications to national and Alliance security and are willing to pay the price for it. With the IoT connectivity rates facilitated by 5G technology, it will also be necessary to look at the devices, applications and software at the end-user side and implement supply chain risk management measures in these areas. Again, common standards must be applied.

In 2021 the CCDCOE will launch a project looking more closely at the supply chain and network security issues related to the 5G roll-out from technological, political and legal perspectives to facilitate a common understanding among NATO Allies and close partners.

[1] Huawei built more than half of the wireless towers, 70% of the Long-Term Evolution (LTE) mobile broadband network, and more than 50,000km of optical cable networks in over 50 African countries. K4D: The Impact of the Belt and Road Initiative Investment in Digital Connectivity and Information and Communication Technologies on Achieving the SDGs

4. The future of AI and security

AI-enabled technology[2] has the potential to transform modern warfare. Opportunities range across a wealth of military applications from autonomous vehicles, to data-processing in intelligence and decision-assistance and logistics and simulation technologies. Several states have announced a considerable investment in AI for defence purposes, with US AI-related R&D funding extending into billions of dollars annually and the UK funding announcement for a new AI centre. Major emerging themes are summarised below.

Fake News

The development of deepfakes[3] and natural language processing models like Microsoft's OpenAI's GPT-3 could have a destabilising effect on international security. GPT-3, which has over 175 billion parameters, was celebrated due to its complexity and computing power but the technology has also been recognised as a threat in the hands of adversarial actors. Many fear that GPT-3 and other text generators could be used to generate large quantities of fake news, as studies have shown these algorithms can generate fake news even more effectively than humans. It is not farfetched to imagine a scenario in which a hostile actor could use a text generator like GPT-3 to quickly generate large amounts of fake news which could lead to a military conflict by heightening ethnic tensions or convincing a country that an attack is underway. This kind of fake news could be especially dangerous when combined with deepfakes. For instance, imagine a situation in which a hostile actor releases a deepfake showing the US President announcing a nuclear attack on North Korea along with many AI-generated false articles discussing the attack. North Korea, fearing a debilitating strike, may launch its own ICBMs. Or imagine a situation in which an adversary generates an army of social media bots, each of which has an AI-generated deepfake profile picture and publishes AI-generated status updates containing destabilising fake news. These AI-run social media accounts would be more difficult to detect and debunk than a deepfake of a public figure. AI-generated fake news is likely to continue to be a major concern well into the next decade, as any attempt to detect AI manipulation risks raising the bar for attackers, making any detection tools swiftly outdated.

Cybersecurity

AI also has several implications within the cyber domain; for example detecting and mitigating threats to a network by using machine learning to detect anomalous traffic or using machine learning in email spam filters. In a security operations centre (SOC), this allows cyber defence analysts to spend less time monitoring and more time on value-adding tasks; a significant advantage in intelligence processing and a shift that has opportunities to improve the efficiency of national security centres and military SOCs across the world. AI may also be used offensively (through deepfakes, as explored above) or to amplify, automate or evolve cyberattacks. While still infrequent in the wild, it is likely that sophisticated actors will experiment with cutting edge approaches including incorporating machine learning into attack tactics, techniques and procedures. The presentation of Deeplocker in 2018 shows how machine learning may be incorporated into malware. From the concerns of a 'machine vs machine' cyber defence landscape to the vulnerabilities of an AI system to cyberattack, the cyber domain will continue to evolve at pace.

Interoperability and Collaboration

> 'We want to make sure our treaty allies, partners, people that—if we're forced to go to war, we'll go to war with—that they're taking safety and responsible AI very seriously.' (Stephanie Culberson, Joint Artificial Intelligence Centre, US Department of Defense)

[2] AI may refer to a wide range of techniques which refer to 'knowledge based' or 'data based' systems. The AI referred to in this report is predominantly on a subset of current 'data based' systems machine learning capabilities. For an accessible overview on the distinctions between subsets of AI see AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference? and A beginner's guide to artificial intelligence, machine learning, and cognitive computing.

[3] Deepfakes are 'AI-generated fake videos or audio recordings that look and sound like the real thing. They leverage powerful techniques from machine learning (ML) and artificial intelligence (AI) called deep learning to manipulate or create visual and audio content'. Tessian: Deepfakes: What are They and Why are They a Threat?

NATO is one potential platform through which Allies may choose to cooperate on military innovation, beyond a number of active collaborative projects happening between smaller groups of states; for example, France, Greece, Italy and Spain have worked together to develop the nEUROn demonstrator UAV which has several autonomous capabilities.

> 'There are considerable benefits of setting up a transatlantic digital community cooperating on Artificial Intelligence (AI) and emerging and disruptive technologies, where NATO can play a key role as a facilitator for innovation and exchange' (NATO Deputy Secretary General Mircea Geoană)

In September 2020, the US held a two-day dialogue termed the 'AI Partnership for Defense', inviting delegations from 12 other partner nations including the UK, Canada and Australia. Core to the Partnership was the theme of interoperability between Allies, particularly aspects including data-sharing and development. Mark Beall, the Joint Artificial Intelligence Center's Head of Strategy, has stated that he expects the Partnership to grow in number as states willing to collaborate with the US to 'shape what responsible AI looks like'. To date, the US is the only state with public Department of Defense Ethical Principles for Artificial Intelligence, in an area through which international norms and approaches have yet to reach any formal consensus.

5. Ransomware attacks in 2020

In recent years, ransomware attacks have become one of the most common threats. The number of ransomware attacks continued to rise during 2020 with a large number of reported incidents in open sources. The COVID-19 pandemic was the most significant event in 2020 and played a considerable role.

Spring 2020 saw a rise in COVID-19 attacker campaigns, with emails frequently referring to the pandemic – for example, pretending to offer important updates – to encourage receivers to open a link. Themed emails proved a lucrative way for attackers to deliver their ransomware 'product' to a large number of victims. As mentioned above, the COVID-19 pandemic made vaccine development and healthcare organisations common targets for ransomware attacks, where commercial targets (private users, organisations, industrial systems) had been more common in previous years.

There could be several reasons why attackers changed their focus toward healthcare providers and facilities. The first was financial income – maybe perpetrators assumed that hospitals would be more willing than usual to pay a ransom as they were a basic element of the fight against the pandemic and the need to restore functionality of their system was extraordinary. Another motivation could be just to paralyse hospitals, cause more harm and support the pandemic to inflict greater economic losses and a deeper crisis. With research organisations developing vaccines, one likely motivation was for the attacks to slow down research and disadvantage victims in the vaccine development race. The characteristics of the perpetrators thus correspond to both criminals and state-sponsored actors. Involvement of some states has already been reported.

The available analysis shows that a range of vulnerabilities was exploited to deploy ransomware during the attacks including vulnerabilities in browsers, remote access tools and browser plugins. It is thus difficult to formulate one recommendation effective against all attacks. Since attackers increasingly do not just encrypt data but steal and threaten to disclose files, backups are not sufficient to protect against the threat. Perhaps only a responsible approach to patch management and advanced technical security solutions can help. Some governmental entities have also introduced another way to mitigate ransomware activities – a recommendation not to pay the ransom and thus reduce attackers' profit and discourage them from continuing other harmful activities.

Throughout 2020, the attention of these attackers appears to have been focused heavily on the healthcare sector, but if the attacks were to be directed against military targets, the same problems can be expected as the level of technology, personnel and finance is usually the same or similar across the public administration.

For guidance on how to prevent or mitigate ransomware attacks please refer to CCDCOE Library products including the *Malware Reverse Engineering Handbook*. This gives an overview of how to analyse malware executables that are targeting the Windows

platform and presents the most common techniques used in malware investigation including setting up a lab environment, network analysis, behavioural analysis and static and dynamic code analysis. The reader will become familiar with disassemblers, debuggers, sandboxes and system and network monitoring tools. Tips learned from the handbook do not protect before attack but can provide useful information about a malicious code including what vulnerability was exploited, what kind of data the malicious code interacted with and information about persistence and encryption.

A similar product, the *Cyber Investigator's Handbook* is scheduled for 2021. It will provide the cyber community with guidelines on managing and handling an incident. Topics from incident response, forensics, malware analysis and network monitoring will be covered. The handbook should support and speed up the analysis and response to an incident and help prevent any reinvasion.

6. Critical infrastructure: a focal point for attacks in 2020

Last year was shaped by an increase in cyber events against critical infrastructure (CI). From the political to the tactical level, different organisations have stressed the importance of the protection of CI. The COVID-19 pandemic has opened possibilities for malicious actors to target critical infrastructure including, for example, the rise of ransomware attacks against German and US hospitals covered in previous issues. Teleworking, spear-phishing and defacement have presented opportunities for malicious actors to disrupt or to get control of IT, operational technology (OT)[4] and industrial control systems (ICS). These examples underline the need for enforcing best practices to defend networks and improve cooperation between stakeholders.

> 'There is no difference between civilian security and military strength, they're one and the same.' (Building transatlantic resilience: Why critical infrastructure is a matter of national security)

Attacks against CI may have political implications. Both NATO and EU leaders have stated that harming CI is unacceptable and that partners and allies will stand in unity against such malicious activities. The US National Security Agency (NSA) has warned of a perfect storm as a consequence of the remote management of systems, decentralised workforces, expanded outsourcing and outdated software. Cyberspace is not limited by geographical boundaries and the resulting interconnectivity and interdependency between friendly and hostile networks and systems provide many vectors for CI attacks.

CI attacks need sophisticated planning and resources. Although the general orientation of the cybercriminal is that of financial enrichment through utility providers,[5] main threats against CI could be categorised as advanced persistent threats (APT),[6] mercenaries and possibly state-backed proxies. According to Microsoft, state actors often target Non-Governmental Organisations and there has been an increase in cyberattacks against IT service providers. A recent example of this, although not directly against CI, is the SolarWinds supply chain compromise discussed above, where a private company was attacked in order to breach the government's protected IT systems. It can be assumed that APTs have some reservations about disclosing and using much of the information they have about state networks and critical infrastructure, as this may have its usefulness on a later and probably more serious occasion. In the meantime, the most attacked critical infrastructure sector is ICT infrastructure.[7]

[4] Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLC) etc.
[5] For example, see Recent Cyber Events #6, October 2020.
[6] Meanwhile Microsoft Digital Defence Report from September 2020 states: 'Interestingly, nation state activity is significantly more likely to target organisations outside of the critical infrastructure sectors. The most frequently targeted sector has been non-governmental organisations (NGOs), such as advocacy groups, human rights organisations, non-profit organisations and think tanks focused on public policy, international affairs, or security.'
[7] 'Within the critical infrastructure sectors, targeting of IT organisations represents over 60% of nation state activity, followed by commercial facilities, critical manufacturing, financial services, and the defense industrial base.' Microsoft Digital Defence Report from September 2020 (p 46)

2020 highlighted how cyberattacks can take shape in a conflict situation. The Nagorno Karabahk conflict showed that CI attacks can be used to inflict distress on governments and populations, a practice in line with ideas of military theorists such as Douhet and Trehnchard, who depicted a quick victory through inflicting damage on morale of society as whole. The situation also raises questions about the protection of society as a whole and what the military's role should be in times of crisis and the protection of national critical infrastructure.

2020 saw a fusion of criminal activity with the tactical use of cyber elements. Examples of this are high profile attacks against water treatment plants in Israel, where reports state that attackers attempted to change the injection of treatment chemicals to unsafe levels. According to media sources, Iranian cyber actors were behind this attack. These types of incidents can lead to casualties within the population[8] and, in a military context, may directly impact the execution of operations because of the fundamental reliance on civilian critical infrastructure, while also raising legal questions.

The Iranian port of Shahid Rajaee was the victim of a cyberattack in May. The attack caused significant disruption to port traffic that lasted at least several days. In this case, the media reported that Israel was behind this attack. Ports, railroads, airports, locks and bridges are critical to military mobility, all depend on cyber infrastructure in one way or another and all vulnerable to cyberattack.

Although there may be no active disruptive attacks against NATO's or allies' critical infrastructure at the moment, compromises that are part of preparations for such attacks may be ongoing. German intelligence and security agencies have reportedly warned about the activities of the Russian-linked hacking group 'Berserk Bear' against companies in the energy, water and power sectors. Such attacks could include reconnaissance, getting and maintaining a foothold for future operations in the targeted infrastructure.[9]

Attacks against civilian infrastructure will potentially affect military operations. It is a national security interest to protect critical infrastructure, as this is a foundation for both civilian and military capabilities and will be targeted using cyber means in a hybrid conflict. Besides good business continuity and disaster recovery plans, it is necessary to invest in training, exercises and effective information sharing between military and civilian actors.[10]

In light of the distribution of COVID-19 vaccine in 2021, it is becoming important to assure the cybersecurity of the full distribution network. In some countries, distribution has been entrusted to military authorities which requires, besides setting up a sophisticated logistical system, consideration of supply chain security from a cyber perspective.

It is therefore important to think about the protection of mobility and lines of communication, as these will give access to the Joint Operations Area (JOA) and keep open timely support options when needed. It is specifically relevant in the context of Anti-Area/Access Denial (A2AD) situations where a new paradigm of multi-domain operations takes place.

Finally, the meaning of what can be categorised as critical infrastructure may have changed. Critical infrastructures have so far been defined primarily by their property of ensuring the maintenance of the functioning of society. Facilities not previously listed as critical infrastructure such as research institutions and even grocery stores could be added to the list because of their essential nature and the fact that they have become targets. Malicious actors not only intend to spy but also to sabotage research and development. The COVID-19 outbreak showed where societies are weakest and pointed to the crisis that could hit society and the military hardest.[11] Collecting various types of infrastructure under the term critical infrastructure raises the question of whether there is a scientifically sound reason for this or whether it is just done for the sake of assuring a certain level of cybersecurity. It can always

[8] See the public discourse on the September 2020 ransomware attack on a German hospital and on whether the death was a casualty of a cyber-attack, for example AP News: German hospital hacked, patient taken to another city dies

[9] Recent Cyber Events #3, June 2020 (p 5)

[10] For more see Bigelow in 11th International Conference on Cyber Conflict: Silent Battle proceeding (p 191)

[11] See also Recent Cyber Events #2, May 2020 (p 5)

be argued, however, that even if all are not critical, the need for protection is essential.

An in-depth and practical perspective on the subject is provided in the *Cyber Commanders' Handbook* published by the CCDCOE. In the future, an *Incident Responders' Handbook* will also be available, which is particularly relevant for critical and essential infrastructures.

7. 2020: Conclusions from the accelerated digitalisation and the digital workspace

NATO and nations have been talking about a digital transformation for years, and yet 2020 showed us that we were unprepared. Even though global digitalisation took a significant jump forward, it is safe to say that the majority of organisations, ranging from NATO Command Structure to COEs, had not accounted for the extensive dependency on IT services needed for business continuity and the additional resources and training this would require.

When a crisis such as the COVID-19 pandemic hits, having contingency plans to ensure business continuity is essential. In a very short time organisations all over the world had to make a swift transition from familiar face-to-face meetings and extensive travel to the home office and online meetings.

A vast range of challenges arise when a crisis forces transition. There are budgetary concerns, questions of what tools, platforms and training are required and every challenge needs to be met while time is of the essence. While trying to identify and meet the needs of the organisation, the change needs to be balanced against a need for a compatible solution that does not violate security protocol and leave the organisation open to new vulnerabilities.

Looking at the CCDCOE's handling of the situation allows parallels to be drawn with other organisations and companies that faced similar challenges over the past year. In the following paragraphs, conclusions are drawn from the accumulated experience of the Centre's lessons learned process and observations about the change of format from a physical conference to an online conference in order to put them in perspective with emerging cyber trends during the pandemic.

Travel had become an integral part of the way we conduct our daily business and had been taken for granted. As soon as the COVID-19 outbreak put an abrupt stop to business travel, many organisations searched for effective ways to substitute traveling and in-person meetings. Thus, connectivity became the number one priority. In 2020, the conduct of business significantly changed as home office and online meetings have overtaken face-to-face meetings.

With a new way of working, new issues arise such as new platforms, new collaboration tools and all of this introduced on the go with little or no training. Many organisations quickly acquired their own platforms or relied on third party services, raising questions of trust and security. With a lack of training for the new working environment, we put ourselves at risk: the absence of an online mind-set is followed by a deficiency of awareness for implicit vulnerabilities.

Key takeaways from the lessons learned these past months have been the importance of a well-established information management system at the workplace that covers all environments and the importance of providing training and supporting the development of an 'online mindset'. Crises require quick reaction but security issues should not be undermined. In the best case, a flexible system is in place that allows for change in times of crisis, while in less optimal cases, course corrections must be made based on problems identified.

Another central theme for 2020 was *trial and error*: For the Cyberspace Operations Discipline, which CCDCOE is leading, organising a big yearly event such as the Annual Discipline Conference fully virtually was an excellent opportunity to learn how to cope in this reality. The lessons identified during the process also apply to online meetings and learning. Two central and sequential challenges that needed to be addressed were platform security issues of *if* a connection can be established and *how* to bring the community together in the virtual space.

Moving online was shaped by the importance of re-designing the content to the medium, mainly keeping it short and simple. In the online environment, less is more. This means shorter sessions, fewer slides, and fewer participants if discussion is desired. There is no easier way to lose a virtual audience than to neglect the need to be extra engaging on your side of the screen. 2020 has not only made us acquire numerous new platforms but

has also made many of us learn new ways of presenting ourselves.

Looking into the future, it is important not to dismiss the security concerns emerging from IT tools and processes we use but to agree on a compromise between usability and security and to anticipate the next crisis with a readiness plan to remain operational and responsive. This means asking the hard questions upfront and learning from this crisis to avoid repeating issues and mistakes.

Central questions that emerged during this pandemic were: 'Does my video-teleconferencing tool work for communication with colleagues outside my organisation?' and 'Can I access necessary documents from outside networks?' Establishing clear security policies on whether and how third-party and off-premise technology and software may be used and building the capability to fall back on tools and services during a crisis by implementing double-use possibilities for everyday equipment and services by factoring-in usability outside the traditional office setting while remaining secure.

Previous issues

This paper is part of a series of monthly reports. This issue as well as all previous issues are available in the CCDCOE online library.

Feedback

To continuously improve this regular report, input from readers is essential. CCDCOE encourages feedback on both how the reports are of use to you and how you think they can be made better.

Please send your comments and suggestions to feedback@ccdcoe.org