CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Recent Cyber Events and Possible Implications for Armed Forces

#6 – October 2020

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 the previous month, 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. Targeted threats against the military and national security

Wearable tokens can make authentication less distracting

'The U.S. Army's wearable authentication tokens intended for the tactical environment could be used for nontactical purposes, such as accessing strategic-level systems, enterprise networks and medical systems, researchers say. ' (AFCEA Signal, September 2020)

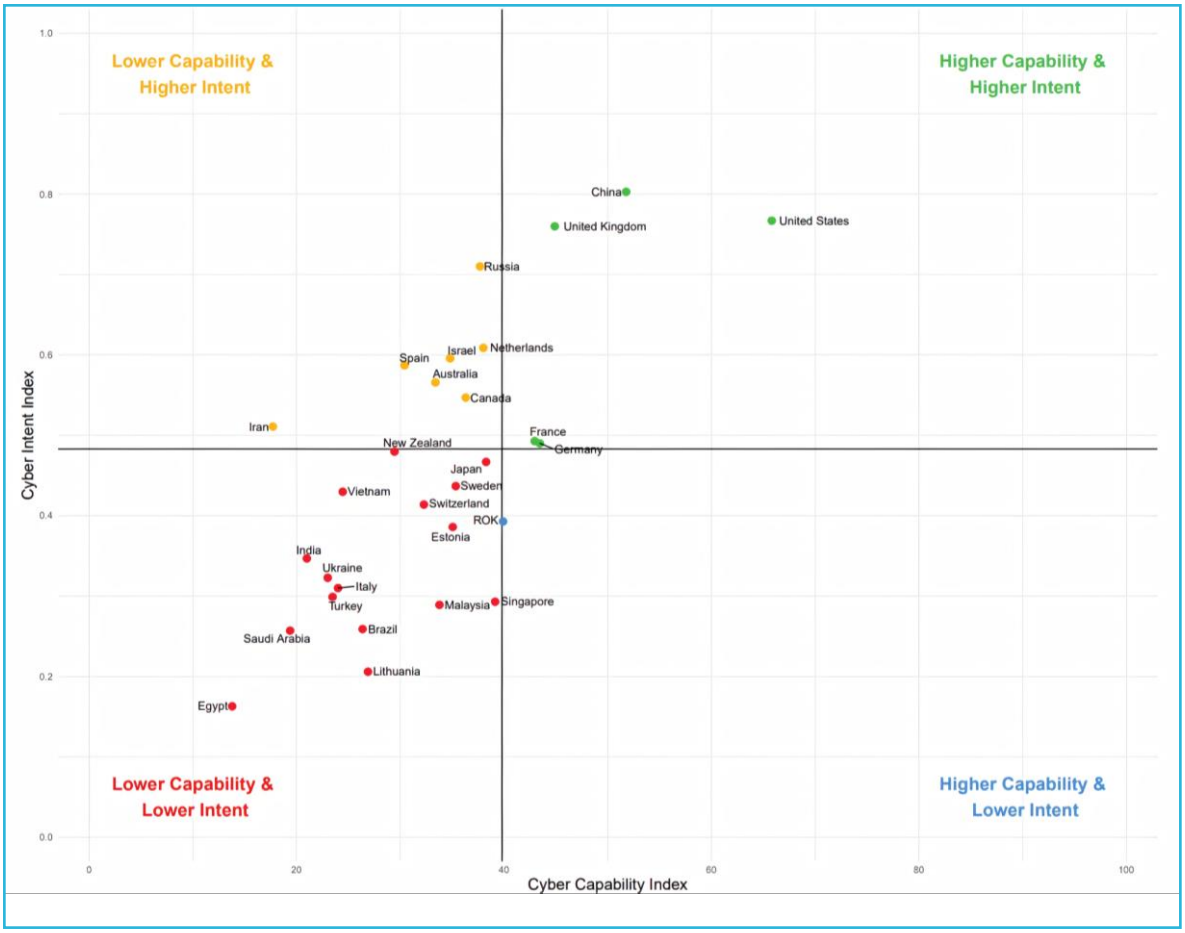
Communication and information systems called tactical networks are essential for supporting the modern armed forces. They aim to provide an extensive range of services, such as: command, control, communications, computers, cyber, intelligence, surveillance and reconnaissance (C5ISR). Access to that system has been quite difficult since soldiers need to use a keyboard to log in and out when needed, which keeps them occupied by the keyboard and not with the battlefield. Since 2017, the US has been developing wearable authentication[1] which seeks to be useable for the soldier in the field, but is also being considered for use outside the tactical environment.

Wearable identity authentication and authorisation technology will be based on wireless technology built into a small token that can be attached to the uniform or worn as a wristband. A second factor, such as a personal identification number or a fingerprint, will complement the token when logging in. The wearable technology will allow soldiers to be more focused to the battlefield than on the keyboard since automatic logout is provided and the use of the keyboard will only be needed for the first login or when a soldier comes back to the equipment. However, this solution is raising some concerns and challenges. For example: secure wireless connection, protection of bio-metrical data, upgrades and updates of equipment and losing the wearable access card. Therefore, it is necessary to make a thorough risk assessment and to mitigate the risks identified.

Belfer National Cyber Power Index (NCPI) released

'In contrast to existing cyber-related indices, we believe there is no single measure of cyber power. Cyber Power is made up of multiple components and should be considered in the context of a country's national objectives.' (Belfer Center, September 2020)

[1] Army Times: Wearable ID to give soldiers access to networks downrange, do more than smartcards



Graph from Julia Voo, et al., 'National Cyber Power Index 2020, Methodology and analytical considerations', Belfer Center, 2020.

A report ranking and detailing the capabilities of 30 states has been released by the Harvard Kennedy School's Belfer Center. The NCPI report aggregates 32 intent indicators and 27 capability indicators to indicate a 'Top 10' ranking of state actors by cyber power of which the US, China and the UK are placed 1st, 2nd and 3rd respectively.

Relying on publicly available data, the report acknowledges potential limitations; for example, underestimating the cyber capabilities of states with significant covert capabilities, such as Israel. The Index provides a comprehensive snapshot of current capabilities across both offensive and defensive cyber capabilities and may be useful for strategic decision-making related to national security matters and the cyber domain and military cyber defence.

2. Other cyber activities relevant to the military

What is a trusted vendor?

'So, basically, the FCC should rely on a pinky swear, cross-your-heart-and-hope-to-die promise from vendors that their equipment is secure. If only Huawei had thought of that.' (Light Reading, 6 September 2020)

The quote is provocative and refers to the Rural Wireless Association's suggestion that vendors should simply certify that their equipment complies with the law to be put on a list of trusted vendors by the US Federal Communications Commission (FCC). But the fact remains that the strategy of the US and others relies on trying to determine which suppliers and equipment can be trusted, and with the complex supply-chains of today, it will be next to impossible to do through vetting. You may have a high level of trust for a domestic vendor, but evaluating all the foreign components that go into that product, or even tracing every subcomponent's origin, is often

beyond the vendor's capacity. This problem will not only face authorities approving equipment for 5G networks but any organisation trying to build secure computing and communication systems. Recent research shows that supply chain risks are major and increasing risks for most organisations and that vendors are often not monitored. [2] Military organisations, often procuring bespoke information systems and using their own communication infrastructure, also need to be able to make these assessments.

Different types of independent assessments and certifications may be one piece of the puzzle when trying to manage these risks, but certification comes with its own pitfalls. First, you have to establish trust in the entity that does the certification. This is admittedly often easier than trusting a vendor, but it can still be a challenge. Then you need to understand the scope and objective of the specific certification and assess if it is appropriate and covers your security requirements. After that, you still need to be prepared for the cases where something is missed in the certification process, and a vulnerability slips through the net.

A comprehensive solution must therefore include several components, and consider the reputation of suppliers, any approvals and certifications available and your own testing, verification and monitoring. The measures should always be proportional to the criticality of the product for the security of your operations.

US company's technology used to cause internet blackout during Belarus protests

'The government used Sandvine's technology to block people from accessing social media websites such as Facebook and Twitter, messaging apps such as WhatsApp and Telegram, and international news websites, Bloomberg reported last month.' (Bloomberg, 11 September 2020)

US-based company Sandvine Inc. reportedly sold network equipment to Belarus authorities which allows filtering of the country's online traffic. The equipment was supplied through a Russian company called Jet Infosystems. [3] According to news articles, Sandvine will now stop working with Belarus and has conducted an investigation, the preliminary results of which indicate that a custom code was used with the company's equipment.

VPN providers and social networks reported that they noticed disruptions during demonstrations in Belarus following the election, and a US Senator is reportedly calling for a US Treasury investigation into Sandvine to determine if the company has violated sanctions. Sandvine's spokespeople are reportedly denying violation of sanctions and state that they abhor the use of technology to suppress the free flow of information resulting in human right violations.[4] According to an investigation by human rights organisation Human Constant and the Qurium Media Foundation, the blocking of the internet was not done on a central level but rather through the nation's individual providers' infrastructure.[5]

The Citizen Lab investigated Sadnvine's product Network Deep Packet Inspection in 2018 and expressed human right concerns over its application. For example, in Egypt, the technology was used to redirect users to ads and cryptocurrency mining scripts and devices allegedly matching Sandvine's PacketLogic fingerprint assumed to be used to block content related to politics, journalism and human rights. According to Citizens Lab, Sandvine's PacketLogic seems to be supporting in-path network injection which could be used to inject spyware. [6]

The use of Sandvine products has shown how those who control the national infrastructure could use their capabilities to influence the flow of information on the internet, redirect it and even bring it to a standstill. While ethical issues for the private industries supporting foreign governments are raised, the public and legal discourse about human rights issues and Sandvine's potential violation of sanctions

[2] SC Magazine: Supply chain weak security link for 92 percent of US companies
[3] 112.UA: US company admitted its involvement in Internet blocking in Belarus
[4] CyberScoop: Networking firm Sandvine cancels Belarus contract, citing 'custom code' that aided censorship
[5] Qurium: How do providers implement Internet blocking in Belarus?
[6] The Citizen Lab: Sandvine's packetlogic devices used to deploy government spyware in Turkey and redirect Egyptian users to affiliate ads?

will be interesting to follow. Incidents like the supposed decentralised internet blocking in Belarus or rerouting of traffic could be viewed as a demonstration of disruptive capabilities, which in this case targeted civilians, but tailored cyber operations could make use of similar methods to target the military considering the military's often strong dependency on civilian and economic networks and infrastructures.

Using SMS for two-factor authentication may be risky

'Researchers have uncovered a threat group launching surveillance campaigns that target victims' personal device data, browser credentials and Telegram messaging application files. One notable tool in the group's arsenal is an Android malware that collects all two-factor authentication (2FA) security codes sent to devices, sniffs out Telegram credentials and launches Google account phishing attacks' (Threatpost, 21 September 2020)

According to news outlets, an Iranian hacker group has managed to develop malware for the Android smartphone operating system which allows interception and theft of two-factor authentication codes (2FA) transmitted through SMS. The 2FA codes for Google, Telegram and social media accounts arriving on the Android phone via SMS could be intercepted and automatically forwarded to the hackers. The malware was hidden inside an Android app and it was probably used in combination with a Google phishing site to obtain user information like username and password.[7]

While 2FA generally increases security and heightens the barrier for malicious actors to gain access to user accounts, SMS is not necessarily the best method for 2FA since it is unencrypted and can be intercepted by other means. Alternatives used by Google, banks and other platforms include, for example, one-time-password (OTP) managers, push-based 2FA, authenticator apps and physical security keys. Some of these alternatives offer additional security features like encryption and passwords, fingerprints and face recognition before allowing access.

With this malware, hackers would only gain access to accounts if they also managed to phish the user's username and password. This means that cyber awareness and vigilance are, next to safe and thought-through 2FA methods, still key to account safety. Individuals working in the government and military sectors can become targets and are advised to exercise caution for social engineering and to generally refrain from mixing private and work online.

It is not recommended to use private email or online cloud storage (Google Drive, iCloud, Dropbox, etc.) or a private phone for authentication instead of services and equipment provided by the employer for work purposes, especially for sensitive data and communication. If the personal account is compromised, work-related data and the communications stored on it may fall into the hands of malicious actors without the knowledge of the employer. Even if exercising good cyber hygiene, online platforms can be subject to hacking and thus data and communications could be leaked without the involvement of the account owner.

Legitimate cloud-monitoring software used as a backdoor

'[A] recently uncovered hacking group, is weaponizing Weave Scope, a legitimate cloud monitoring tool, to help install cryptominers in cloud environments, according to reports from Microsoft and Intezer. […] Over the past several months, researchers have uncovered a number of cryptomining campaigns targeting cloud platforms and containers.' (Data Breach Today, 10 September 2020)

According to reports from Microsoft and Intezer, a recently uncovered hacking group is using a legitimate cloud-monitoring tool to get access and install malicious code in cloud environments.[8] The most important aspect of this type of attack is the capture of cloud resources for malicious activities such as cryptomining [9] using legitimate software without the need for any attack tools. 'By

[7] ZDNet: Iranian hacker group developed Android malware to steal 2FA SMS codes
[8] Microsoft: TeamTNT activity targets Weave Scope deployments, Intenzer: Attackers abusing legitimate cloud monitoring tools to conduct cyber attacks
[9] Cryptomining is the process of computational work (solving complex mathematical problems) in order to gain cryptocurrency. See also Wikipedia.

installing a legitimate tool such as Weave Scope, the attackers reap all the benefits as if they had installed a backdoor on the server with significantly less effort and without needing to use malware,' Nicole Fishbein, a malware researcher at Intezer, notes in the report.

Nowadays, many countries are looking for ways to migrate to cloud architecture due to ease of management and cost-effectiveness. However, this attack type revealed once again that security analysis and configurations of cloud architecture must be done meticulously.

Learn which phishing tricks users still fall for

Phishing is still one of the most effective attack vectors to gain remote access to victim's system – no cost for 0-day vulnerability research and exploit development, just a nice email which convinces the user to visit a fake webpage, fill in credentials in a fake form, download a malicious file or open a malicious attachment.

Sophos has published this year's results of their customers' reactions to a phishing attack simulator. It indicates what emails are dangerous and when phishing is successful.

'The answers covered a broad range of phishing themes, but had a common thread: not one of them was a threat. Most of them dealt with issues that were mundane and undramatic, while at the same time apparently being interesting, important, or both. Nothing on this list was truly urgent or terrifying, and they all sounded likely and uncomplicated enough to be worth getting out of the way quickly.' (Naked Security by Sophos, 4 September 2020).

Themes such as rules of conduct, delayed year-end tax summary, scheduled server maintenance, task assigned to you, new email system test and vacation policy update came top. Ordinary messages common for every day, no breathtaking news nor gift offers. Fake daily routine internal communication was the worst.

To reduce the risk of compromise, end-user education should be provided where the following ideas can be presented:

- Check the sender's address and contact them via another communications channel if any doubts.
- Check links before clicking – an attacker may use a domain name similar to the real organisation's one (for example 'o' replaced by zero in 'google').
- Notice other strange signs such as spelling mistakes, weird terminology, software tools your organisation doesn't use and appeals to unusual behaviour (alter security settings; provide credentials; download, open or run a file).

When phishing is targeted (so-called spear-phishing) against high-level decision-makers, their assistants or co-workers, the resulting damage can be especially serious. Even if only unclassified accounts of senior military officers are breached, valuable information may be revealed, and the compromised accounts may be used to deceive others. The awareness of this threat is therefore important at all levels.

3. Policy and strategy developments

Patient dies as a result of a ransomware attack

'German authorities said Thursday that an apparently misdirected ransomware attack caused the failure of IT systems at a major hospital in Duesseldorf, and a woman who needed urgent admission died after she had to be taken to another city for treatment.' (Associated Press, 17 September 2020)

A recent upsurge in cyberattacks on health-care providers worldwide including in France,[10] Spain,[11] Thailand,[12] the US[13] and the Czech Republic,[14] together with the COVID-19 pandemic, underline the importance of cybersecurity in the health-care

[10] ITProPortal: Paris hospitals targeted in major cyberattack
[11] MurciaToday: Cyber-attack threatens Spanish hospital computer systems
[12] BitDefender: 5 Times more Coronavirus-themed malware reports during March
[13] NBC News: Major hospital system hit with cyberattack, potentially largest in U.S. history
[14] CyberScoop: Czech Republic's second-biggest hospital is hit by cyberattack

sector and of understanding what protection the existing law offers.

Under international law, which by definition only regulates actions attributable to states, several regimes can apply to a cyber operation, depending on its context. During armed conflict, extensive protection is granted to health care by international humanitarian law which requires medical services and facilities to be protected at all times by the parties to the conflict. NATO and like-minded states hold that this also applies in cyberspace. In planning cyber operations, the military must thus take all the precautions and assume all responsibilities they would have concerning kinetic operations.

Outside armed conflict, other legal concepts, namely sovereignty, the principle of non-intervention and the prohibition of the use of force, are applicable, depending also on the legal views of individual states. International human rights law is also relevant since it has been affirmed that the same human rights must be protected online and offline.[15] Calls for a new norm specifically protecting the health-care sector have been made.[16] While this may be a long-haul ambition, states have been quite unequivocal in their condemnation of such cyberattacks, as have NATO and the EU.

Of course, cyber security starts with one's own responsibility. Several countries have included hospitals and other medical facilities among critical information infrastructure and a failure to adequately protect them from cyberattacks may be found to violate national law. Nonetheless, no deficiency on the part of information system administrators absolves an attacker of responsibility for their actions. No less than 65 states have committed to adopting national legislation penalising computer crimes including attacks on information systems under the Budapest Convention on Cybercrime.

Not only ethics but also the law is thus clear about the unacceptability of cyber operations against the health-care sector.

4. Recent guidelines and recommendations

NSA guidelines help DOD employees and others to work securely from home

'Should the indicators of compromise outlined in the document be observed, users are advised to apply the provided mitigations to any computer, mobile device, or IoT device connected to their personal network.' (SecurityWeek, 21 September)

On 17 September, the NSA has published two security guidelines, called cybersecurity information sheets (CSIs), concerning the work-from-home environment. The first CSI, entitled 'Compromised Personal Network Indicators and Mitigations', provides a list of indicators of compromise and the recommended actions for mitigation, useful for end-users in monitoring and managing their own equipment. While this document is primarily intended to help users of National Security Systems (NSS) and Department of Defense (DOD) employees identify and mitigate the compromise of their personal or home networks, it can, as the NSA points out on its website, be useful in preventing compromises on any network.[17]

The second CSI, 'Performing Out-of-Band Network Management' is for systems administrators. It provides an overview of network segmentation between management and user traffic to prevent compromised user devices from compromising network infrastructure and a series of recommendations for hardening network security.

Last April, the NSA published another security guideline for the teleworking environment, 'Selecting and Safely Using Collaboration Services for Telework'.[18] It provided a list of security criteria for government/military to consider and assessment results for 17 commercial collaboration services such as Cisco Webex and Microsoft Teams.

[15] Council of Europe: Guide to human rights for Internet users
[16] ICRC: Norms for responsible State behavior on cyber operations should build on international law
[17] NSA CSS: Reduce Risk of Network Compromises
[18] NSA CSS: Working from Home? Select and Use Collaboration Services More Securely

Russia proposes Cyberspace Truce

'President Vladimir V. Putin of Russia on Friday proposed a truce with the United States in cyberspace, without acknowledging that his country has repeatedly used cybertechniques to attack elections from the Ukraine to the United States, stolen emails from the Defense Department to the White House, and developed some of the world's most sophisticated disinformation efforts.' (*The New York Times*, 25th of September 2020)

President Putin reportedly issued a written statement containing a four-point plan that aims to agree on: (1) restoration of regular full-scale bilateral interagency high-level dialogue; (2) maintaining continuous and effective communication channels between the states' competent agencies; (3) development of a bilateral intergovernmental agreement on preventing incidents in the information space; and (4) exchange of guarantees of non-intervention in internal affairs, including the electoral process.[19]

According to the New York Times, President Putin did not make any concessions on Russia's alleged accelerated use of cyber weapons in the past. Russia also denies that they have meddled in US elections in the past. National Security Council spokesperson John Ullyot reportedly dismissed Russia's offer and said: 'It is hard to take such statements seriously when Russia, China, Iran and others have sought to undermine our election process.'[20] The Wall Street Journal reported at the beginning of September that Microsoft's threat intelligence teams saw Russian hackers target around 200 organisations with ties to this year's US presidential election.[21]

In 2017 President Trump tweeted about a discussion between him and President Putin forming a cyber-security unit addressing, among other things, election hacking. While Trump's tweets were not met with much approval from cybersecurity experts, they became relevant again in 2018 when the two world leaders met in Helsinki, and President Putin reportedly proposed the countries work together examining evidence that Russia had meddled in the US presidential election. [22]

A comprehensive overview and analysis of Russia's cyber strategy and forces by Bilyana Lilly and Joe Cheravitch can be found in the 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade.

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

[19] President of Russia: Statement by President of Russia Vladimir Putin on a comprehensive program of measures for restoring the Russia – US cooperation in the field of international information security

[20] *The New York Times*: Putin wants a truce in cyberspace — while denying Russian interference

[21] *The Wall Street Journal*: Russian hackers have targeted 200 groups tied to U.S. election, Microsoft says

[22] Politico: Trump-Putin meeting rekindles ridiculed cyber plan