CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Recent Cyber Events and Possible Implications for Armed Forces

#5 – September 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

Consolidating the 'new normal'

'NATO's cybersecurity chief has admitted that the agency ran through contingency plans A, B, C and D to cope with the impact of the Covid-19 outbreak, as he also conceded that systems, protocol and planning may never come back as they once were. Like many who prefer to describe a 'new normal' as opposed to a return to 'business as usual', Ian West described how the planning for NATO's facilities around the world was fundamentally exposed - as has been the case for many organisations around the world. Addressing the virtual conference, West said NATO was as relevant to any discussion on 'progressing beyond this new normal' as any other nation, government or organisation because it was "significantly impacted" by the pandemic.' (SC Magazine UK, 1 July 2020)

The COVID-19 pandemic has challenged the modus operandi of many enterprises and organisations worldwide, resulting in measures taken to keep personnel safe and adhere to respective national guidelines, all while remaining operational. The consequences of this have varied. Twitter realised that working from home can be effective and will now allow staff to work from home indefinitely,[1] while streaming services Netflix and YouTube reportedly reduced the quality on their platforms in Europe to minimise load on the internet.[2] The underlying fact is that home office and rotational staffing of offices takes advantage of the internet and CIS infrastructures at a magnitude never before seen and it seems like the pandemic has enabled new opportunities in the digital word and challenges alike. With a rise in demand for and use of digital collaboration tools, security requirements, process and procedures rise symmetrically.

These challenges are also faced by NATO, as Cyber Security Centre Chief Ian West reportedly addressed during the SC Media UK digital congress. Not returning to offices puts demands on CIS infrastructure, and to enable staff to work from home, hundreds of laptops, tablets and smartphones have had to be issued in a short time.[3] In July, NATO Policy Directors for Civil Preparedness held a video conference discussing COVID19 and how to strengthen national resilience and update baseline requirements to prepare for further pandemic waves.[4]

[1] BBC: Coronavirus: Twitter allows staff to work from home 'forever'[2] CNN: Netflix and YouTube are slowing down in Europe to keep the internet from breaking

[2] CNN: Netflix and YouTube are slowing down in Europe to keep the internet from breaking

[3] SC Magazine UK: SC Digital Congress: NATO cybersecurity chief: 'We may never return to offices 100 per cent'

[4] NATO: NATO Policy Directors discuss strengthening resilience and preparations for second wave in the COVID-19 pandemic

Whether or not the workplace reality which the world is now facing is the new normal or is an aberration, learning from how events have unfolded and determining the requirements to guarantee continuity of operations must not only result in preparedness concerning the availability and operability of necessary CIS equipment, but also in proactive and feasible security policies, process and procedures. Policy and regulatory preparedness should affect important security questions such as the implications of relying on third-party off-premise communication tools and how interoperability between organisations and entities can be accomplished without jeopardising security or enabling shadow IT.

Cyber means used to spread disinformation about NATO

'A disinfo operation broke into the content management systems of Eastern European media outlets in a campaign to spread misinformation about NATO. […] In some cases, FireEye says, Ghostwriter has deployed a bolder tactic: hacking the content management systems of news websites to post their own stories. They then disseminate their literal fake news with spoofed emails, social media, and even op-eds the propagandists write on other sites that accept user-generated content.' (Wired, 29 July 2020)

Not only is the tactic used in the case related above much more aggressive and more difficult for the public to detect as disinformation, of particular concern for militaries is that the disinformation concerns NATO. When the content of disinformation campaigns specifically targets the credibility of military organisations, those organisations need to take part in countering the information operations.

The tactic to hack news outlets and corrupt and manipulate their content is particularly worrying since the reputation of news sources is an important factor for the public in assessing the reliability of the information. Fake information trumpeted through a previously dependable channel will have a good chance of delivering the desired effect.

News outlets need to be prepared for this type of campaign and be able to increase their security, perhaps with increased government support, and their communications around these issues. Awareness amongst the general public that this tactic is being used, and that even news from legitimate outlets may be manipulated, also needs to be increased. One way to work towards this this would be a governmental confirmation mechanism for information that would reference official communication channels. News outlets and the public could trace back the origin of referenced information and thus determine possible misinformation campaigns effectively and efficiently.

It is also worth mentioning the developments in artificial intelligence and machine learning that may make disinformation much more difficult to spot in the future. Machine learning technology can be used in the production of so-called deepfakes, highly realistic fake images and videos. The technology could make disinformation campaigns much more effective, with videos featuring prominent individuals seemingly endorsing the adversary's narrative.[5]

Deepfake creation is not difficult and will become even easier with time. The material costs are not prohibitively high, and much of the know-how is published openly and available to use. Costs will continue to decline as research advances continue to be distilled into easy-to-use software and open-source code. However, detection systems and takedown policies will help to keep commodified deepfake technologies at bay to a certain extent. Microsoft, for example, recently announced new technologies to combat disinformation including software too analyse video for signs of manipulation.[6] The greater threat will be from tailored, targeted fakes: the trends indicate that these hoaxes will remain a persistent threat.

North Korean APT conducting espionage in the defence sector in Israel

'Israel said […] it thwarted a cyberattack on its defence industry by a hacking group known as Lazarus, which the United States says is run by North Korean intelligence. Israel's Defence

[5] CSET: Deepfakes: A grounded threat assessment

[6] Microsoft: New Steps to Combat Disinformation

Ministry said hackers posing as potential employers sent job offers to defence workers trying to infiltrate their networks and gather sensitive information. The group built fake profiles on the LinkedIn network to disguise its hackers […]' (Reuters, 12 August 2020)

Since at least 2009, North Korea has been linked to many different kinds of cyberattack around the globe, including the Sony Pictures hack in 2014, the Bangladesh bank heist in 2016, the WannaCry ransomware in 2017 and various cryptocurrency attacks afterwards. In the latest attack on an Israeli defence company, Lazarus allegedly tried to deceive employees of the defence companies by impersonating CEOs and personnel managers offering good positions.

North Korean hackers have used this 'job offering and seeking' strategy for years. On 20 July 2020, McAfee reported that North Korean hackers had used a series of malicious documents containing job postings taken from leading defence contractors. The documents used as lures offer positions for work with specific US defence programmes and groups, such as the F-22 programme and Defence, Space and Security (DSS).[7]

CISA and FBI have published an analysis report on malware variants reportedly used by the North Korean government in this type of attack.[8] Militaries of NATO member nations have a long tradition of collaboration with industry in the private sector. As the infiltration into military and related government organisations is becoming harder, the targets of cyber actors are gradually moving to those parts of military industry and academia that hold confidential information. To defend against this kind of attack, security awareness is of the utmost importance and sound technical security measures should be implemented to prevent and detect malicious documents and hosts. Such security awareness programmes ought not only to cover cyber hygiene at work, but also for work at home and even in the personal sphere, as in the cyber domain the distinction between the private and professional is often blurred, and attackers choose the most vulnerable point for attack.

A space-based system as an anti-satellite weapon

'According to a July 23 SPACECOM statement, Russian inspector satellite Cosmos 2543 released another object into space in proximity to another Russian satellite, an action inconsistent with its stated purpose. U.S. officials have suggested in the past that such an object could be used as a high-speed projectile weapon to attack other satellites.' (C4ISRNET, 23 July 2020)

The anti-satellite weapons (ASAT) is nothing new, but we need to consider this type of weapon as very dangerous in the modern digital age. In the modern world, space-based capabilities provide all kinds of support to military, commercial and civilian applications, and they are key to intercontinental communication and information exchange.

There are three categories of targeted satellites: navigation, communication and reconnaissance, and tactical. ASAT can employ an electro-magnetic pulse device, kinetic weapon or intercept and jam communication systems on any of them.[9] Bussert believes that ASATs pose the greatest threat to cyberspace and the greatest cyber threat.[10] Therefore we can expect states to build offensive cyber capabilities which can be repurposed for ASAT attacks.[11]

According to an article from C4ISRNET, Russia continues developing a satellite system able to be used as an in-orbit weapon. That type of ASAT presents a high threat to the modern world and to NATO and its member states which use sophisticated information and communication systems from the tactical to the strategic levels. The loss of a satellite for the country or NATO could thus lead to information collapse in the commercial or military domains. This could result in the loss of the C4ISR capabilities necessary for peacekeeping and military operations. To mitigate this threat, NATO and its member states must build in redundancy using

[7] McAfee : Operation North Star – A job offer that's too good to be true?
[8] CISA: Malware analysis report (AR20-232A) - North Korean remote access arojan: BLINDINGCAN
[9] Bussiness Today: What is ASAT and how can it be used in war?
[10] AFCEA SIGNAL: Antisatellite Weapons pose major cyberthreat
[11] The Cyber-ASAT: On the impact of cyber weapons in outer space

terrestrial systems for C4 and for the international community to make an agreement limiting ASAT.

2. Other cyber activities relevant to the military

Vulnerabilities in VPN for Operational Technology

‘Researchers have discovered remote code execution vulnerabilities affecting virtual private network (VPN) implementations primarily used to provide remote access to operational technology (OT) networks. […] This kind of access has become especially prioritised in recent months due to the new reality of the COVID-19.’ (Claroty, 28 July 2020)

Remote connections to OT[12] networks should be strictly managed to prevent security incidents resulting from external unauthorised access. Where the highest level of security is required, such as in safety-critical systems, remote maintenance may not even be allowed by security policies or regulations. However, on-site maintenance with face-to-face contact has become more difficult due to the COVID-19 pandemic and remote maintenance could be regarded as more attractive than ever.

If remote access is absolutely required for maintenance, it should be enabled on an as-needed basis and its connection should be monitored properly. It is also important to apply the latest security patches, of which stability and compatibility have been confirmed by vendors, to mitigate security risks surrounding the remote access environment including the VPN connection. Critical infrastructure operators should also periodically check for new vulnerabilities that could be exploited by cyber actors to infiltrate industrial control systems. Since properly functioning critical infrastructure is an enabler for modern military operations, liaising with operators is important to the armed forces.

Advisories and reports from CSIRTs and vendors can be good references. Best practices such as the guidelines published by the US Department for Homeland Security (DHS) [13] and German Federal Office for Information Security (BSI) [14] can be consulted to ensure secure remote access for industrial control systems.

3. Policy and strategy developments

Different strategies concerning 5G and China

‘The U.S.'s latest salvo against Huawei is creating headaches for European telecom operators locked into contracts with the Chinese telecom giant. Last week, Washington announced it is blocking the use of any American technology in microchips powering Huawei's smartphones and networking equipment, dealing what some analysts called a “lethal blow" to the company’. (Politico, 25 August 2020)

The worldwide preparations for national 5G rollouts remain a significant topic and there are some clear discrepancies in the approach of countries on whether to allow Chinese companies to be part of their infrastructure. India reportedly decided to not include ZTE and Huawei and to quietly phase out existing telecommunication equipment from those companies. [15] The UK has adapted its approach and will remove Huawei equipment completely from its 5G infrastructure by 2027 as a reaction to recent events.[16] France has reportedly decided not to issue a ban on Huawei, but national operators using Huawei will likely only receive limited licenses lasting between three and eight years.[17]

According to news reports, Germany has not yet decided on whether to use Huawei equipment, and the UK’s recent decision

[12] Operational technology (OT) refers to computing and communications systems used to monitor and control physical devices and processes, such as industrial operations, weapons or other tactical systems.

[13] DHS: Remote access for industrial control systems

[14] BSI: Remote maintenance in industrial environments

[15] CNET: India is reportedly phasing out Huawei equipment from its networks

[16] UK Government: Digital, Culture, Media and Sport Secretary's statement on telecoms

[17] SecurityWeek: Huawei not totally banned from France, says watchdog

might affect its thinking.[18] The US continues its campaign against Huawei by trying to stop worldwide use of American hard- and software in and for Huawei designs. Germany's decision on its 5G infrastructure will, according to the Economist, play a vital role for the rest of the European Union. [19] Meanwhile, the US and Israel are working on an MoU to exclude Chinese 5G technology from Israel's 5G network.[20]

While Huawei is currently the most prominent and often cited centre of discussion about 5G infrastructure, the actual problem goes deeper and concerns more than just individual Chinese companies. Even if there are additional threats associated with Huawei, the basis for concern is founded in the legal and strategic framework of China itself. China is determined to become a leader in global high tech manufacturing and has set out its goal in its 'Made in China 2025' policy.[21] To further this goal, and as pointed out in the CCDCOE paper *Huawei, 5G, and China as a Security Threat*, the Chinese National Intelligence Law of 2016 requires all companies 'to support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work'.[22]

On a related note, Chinese-owned apps *TikTok* and *WeChat* will be banned from operating in the USA 45 days after Executive Orders have been issued. The deadline set by President Trump is 15 September, before when *TikTok* must be sold to a US buyer or will be shut down in the country. [23] The Executive Orders are said to ban transactions between the Chinese parent companies *ByteDance* and *Tencent* and any US entities.[24] The developments observed in the greater framework of the US-China trade war are a constant balancing act between national security and economic development and the innovations resulting from it.

President Trump confirms a U.S. cyberattack on a Russian troll farm

'During an Oval Office interview with [columnist Marc A. Thiessen] this week, President Trump acknowledged for the first time that, in 2018, he authorized a covert cyberattack against Russia's Internet Research Agency, the St. Petersburg-based troll farm that spearheaded Russian interference in the 2016 presidential election and was doing the same in the 2018 midterm elections.' (*The Washington Post*, 11 July 2020)

The cyber operation that President Trump recently acknowledged authorising, and the reported ties to US Cyber Command, has now been known for over a year. [25] A public acceptance by the US head of state, of course, simplifies attribution. The cyber operation to thwart Russia's Internet Research Agency's attempts to interfere with US elections is one example of how the US 'Defend Forward' strategy is being implemented and how pre-emptive operations are carried out at part of that strategy. Perhaps Russian reactions over time will provide some clues to whether officially taking responsibility for offensive operations can contribute to deterrence.

An interesting question such an operation raises is what legal constraints apply to such 'anticipatory' operations. There is little debate that a state may respond to coercive interference in its domestic matters which diminishes its political independence – but how? Articles 2(4) and 51 of the UN Charter prohibit the threat or use of force against a state's territorial integrity or political independence, and ensure the right to defend against armed attack, regardless of means,

[18] VOA: After Britain, Germany emerges as next 5G battleground
[19] The Economist: America's war on Huawei nears its endgame
[20] *The Nation*: Israel closer to US 'Clean Network' by abandoning Chinese 5G Technology
[21] Council on Foreign Relations: Is 'Made in China 2025' a threat to global trade?
[22] The Strategist: Australian Strategic Policy Institute: Huawei and the ambiguity of China's intelligence and counter-espionage laws
[23] CNN: Trump issues orders banning TikTok and WeChat from operating in 45 days if they are not sold by Chinese parent companies
[24]The Verge: The big legal questions behind Trump's TikTok and WeChat bans
[25] *The Washington Post*: U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms

and including imminent attack as formulated in the Caroline test.[26]

Below such thresholds, states are navigating several difficult-to-reconcile objectives: the material and procedural boundaries of the law of state responsibility; avoiding further destabilisation in cyberspace; and producing credible deterrence that can influence adversary decision-making (see the lessons from the anti-ISIS campaign)[27]. The credibility of advocating norms of responsible state behaviour in cyberspace is, of course, directly affected by one's own adherence to such norms.

Australia releases a new cybersecurity strategy

' "The Australian government will confront illegal activity, including by using our offensive cyber capabilities against offshore criminals, consistent with international law," it said. "The Australian government will continue to strengthen the defences of its networks, including against threats from sophisticated nation-states and state-sponsored actors." ' (ZDNet, 6 August 2020)

In the July issue of this publication, Australia's response to disinformation campaigns was reported. The Australian government had announced plans to establish the country's first taskforce devoted to fighting disinformation under the Department of Foreign Affairs and Trade.[28]

A new cybersecurity strategy was released by the Australian government on 6 August replacing the former strategy from 2016. The strategy states that cyber incidents and cyber-crimes could have a significant effect on the country's economy and the job market. Investment intended to build up new cybersecurity and law enforcement capabilities are planned.[29] The strategy also announces an investment of $62.3 million in a 'classified national situational awareness capability to better enable government to understand and respond to cyber threats to critical infrastructure and other high priority networks'.[30]

In 2016, former Prime Minister Turnbull confirmed that Australia possesses offensive cyber capabilities and would use them to counter offshore cyber criminals, support military operations and respond to serious cyber incidents against Australian networks.[31]

Apart from the significant investments in cyber capabilities, the nation's critical infrastructure policies will see change and the government will shift to a centralised model of managing cybersecurity for government departments. Businesses can follow a voluntary code of practice for IoT, and bigger businesses will be encouraged to help smaller ones. The government will work with large businesses to provide cybersecurity tools and services.[32]

The *New York Times* reports that tensions between Australia and China are rising and Australia seems to be seeing an increased number of online attacks. While the attacks are reported to be constant, they have seemingly become more troublesome since Australia called for an international inquiry into the origins of the coronavirus pandemic.[33]

US Senate wants more clarity on cyber operations

'The Senate Armed Services Committee is asking the Department of Defense for greater clarity and formalization of its cyber operations.' (The Fifth Domain, 24 June 2020).

The US Senate Armed Services Committee's draft of the National Defence Authorisation Act asks for an assessment of cyber operational planning as well as de-confliction policies and processes by November 2021.

Cyber operations exist in the global domain, where outcomes for national security are not

[26] Oxford Public International Law: The Caroline Incident—1837
[27] C4ISRNET: What Cyber Command's ISIS operations means for the future of information warfare
[28] The Conversation: China's disinformation threat is real. We need better defences against state-based cyber campaigns
[29] Australia's Cyber Security Strategy 2020
[30] Australia's Cyber Security Strategy 2020, page 23.
[31] Australian Strategic Policy Institute: Australia's offensive cyber capability
[32] ZDNet: New Australian cybersecurity strategy will see Canberra get offensive
[33] *The New York Times*: Australia spending nearly $1 billion on cyberdefense as China tensions rise

always visible, parameters for assessment are not well defined and de-confliction between different cyber units is nebulous. This leaves civil leadership uncertain of how best to show cyber strength without losing advantage.[34] From defence capability development beforehand, and regarding ongoing or planned cyber operations, it deems necessary to conduct periodic assessments. The Senate is calling for an assessment focusing on whether policies and processes are appropriate and sufficient for the conduct of timely and effective cyber operations, including whether the targeting cycle is appropriate, relevant intelligence is available and authorities and delegated to the appropriate level.

It is advisable to have a full process (including proper assessment) in place for assessing and de-conflicting national cyber effort for reducing waste and increasing the effectiveness of the resources used. It is also important to ensure that who has the authority to execute cyber operations that may have strategic consequences is clearly defined, that there are mechanisms to coordinate between different agencies and ministries and that this is captured in the relevant national policy and doctrine documents.

4. Recent guidelines and recommendations

The FBI has issued warning over Windows 7 end-of-life

'The FBI has observed cyber criminals targeting computer network infrastructure after an operating system achieves end of life status. Continuing to use Windows 7 within an enterprise may provide cyber criminals access into computer systems. As time passes, Windows 7 becomes more vulnerable to exploitation due to lack of security updates and new vulnerabilities discovered.' (FBI, 3 August 2020)

Operating system Windows 7 reached end-of-life when Microsoft stopped providing support on 14 January 2020. Such an important milestone has brought a serious issue for information systems where the upgrade or replacement process to current and supported operating systems is a complex or even impossible task. This might be due to software backward compatibility or hardware requirements.

According to the FBI,[35] there have been ongoing attacks on Windows 7 targeting recent critical vulnerabilities. Governments and organisations are strongly encouraged to assess the risk of using Windows 7 and to mitigate the potential damage from data leaks, data loss, system malfunction or denial of service. In military systems or other critical information systems the consequences for national security and defence could be severe.

The best way to prevent these problems would be to upgrade or replace unsupported software. Organisations should ensure that this is reflected in directives and internal regulations and develop procedures to implement it. If this is not possible, which may be the case for highly specialised military software that has not been updated to work with newer operating systems, air-gapping[36] of the vulnerable system should be considered. However, this will not close all attack vectors; for example, portable external media in combination with an end-user human factor can still cause a breakdown. If the system cannot be air-gapped, security hardening for example by employing a firewall, monitoring and implementing software security policies will reduce risk.

NSA releases guidelines on limiting location data exposure

'Anything that sends and receives wireless signals has location risks similar to mobile devices. This includes, but is not limited to, fitness trackers, smartwatches, smart medical devices, Internet of Things (IoT) devices, and built-in vehicle communications. Personal and household smart devices (e.g., light bulbs, cookware, thermostats, home security, etc.) often contain wireless capabilities of which the user is unaware. Such IoT devices can be difficult to secure, most have no way to turn off

[34] Help Net Security: Cyberwarfare: The changing role of force

[35] FBI: Computer Network Infrastructure Vulnerable to Windows 7 End of Life Status, Increasing Potential for Cyber Attacks

[36] Air-gapping refers to separating a computer or network of computers so that is has no network connection to the internet or any other systems. The lack of network connections makes such systems more difficult to reach for an attacker.

wireless features, and little, if any, security built in. ' (NSA, 4 August 2020)

On 4 August, the US National Security Agency (NSA) released a guideline on how to limit location data exposure on mobile devices for National Security System (NSS) and Department of Defense (DoD) members. The guide called *Limiting Location Data Exposure* is publicly available and summarises potential risks stemming from exposure of location data and provides measures to minimise and limit sharing of this information.

In summary, the measures are to turn off location services, Bluetooth and Wi-Fi. Additionally, whenever not using the phone, airplane mode can be turned on. Location sharing permission for individual apps should be declined if possible, or set to 'only allow while using the app'. The smartphone's advertising ID should be reset at least in weekly intervals and tracking features like Apple's 'Find My' for iOS devices, Android's 'Find My Device' or any equivalent service should not be used and a trusted VPN should be used whenever possible.[37]

The NSA guideline explains that location services and GPS are not the same and that disabling location services does not turn off GPS nor does it reduce the risk of location exposure. It solely limits access to data by apps but does not limit the operating system from using location data and communicating it. Mobile devices can calculate location with Wi-Fi and Bluetooth if cellular signals and GPS are not available and apps or websites can also use sensor data and browser information. The guideline goes on to state that many apps request permission for location even if it is not needed for the function of the app itself, and warns about sharing information on social media.

Particularly interesting is the NSA recommendations on a mission scenario. If it is critical for a mission that a location is not revealed, it is recommended to identify a non-sensitive location where mobile devices can be secured before the start of activities. Since turning them off might not be enough, devices should be left at this location; this includes personal mobile devices. For transportation, either vehicles without integrated wireless communication capabilities should be used or they should be turned off, if possible.[38]

Minimisation of location data sharing may not be a priority for many units and the security implications of not taking any measures may seem farfetched. While the effects may not be immediate and may not necessarily compromise individual missions, the threats are real. Often, the data from one individual is not significant by itself, but becomes valuable intelligence when put into the right context. Even if third parties and companies seem trustworthy and their affiliations have been checked, leaks and hacks could still expose valuable information stored with them.

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

[37] Wired: Security News This Week: The NSA's Tips to Keep Your Phone From Tracking You

[38] NSA: Limiting Location Data Exposure