CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Recent Cyber Events and Possible Implications for Armed Forces

#2 – May 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, but 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. COVID-19 related news

COVID-19 disinformation continues to spread using social media and other cyber means

'China has systematically spread disinformation about COVID-19 to shift blame for the pandemic, a think tank has claimed'. (*Express*, 5 April 2020)

Crime and disinformation connected with the COVID-19 pandemic continue. Law enforcement agencies warn that state actors like Russia,[1] China and Iran[2] are said to be behind some of these disinformation campaigns. A common theme is to blame the United States for the pandemic. The desired result of this is to cause cracks in the unity of the Alliance.

Conspiracy theories also flourish, like the theories that the roll-out of 5G technology is related to the spread of the virus,[3] which have been reported as leading to mobile masts being attacked and broadband engineers being threatened.[4] State actors are not always the main players in this, but the theories may be fuelled or inspired by state or state-sponsored actors.

Tracing the spread of COVID-19 may mean risks for privacy and security

'Chinese-style surveillance is coming to a neighbourhood near you. From drones barking orders at park-goers to tracking people's movements through cellphones, Western governments are rushing to embrace sophisticated surveillance tools that would have been unthinkable just a few weeks ago. In the European Union, home to the world's strictest privacy regimen, leaders have taken the unprecedented step of asking telecoms companies to hand over mobile phone data so they can track population movements and try to stop the spread'. (Politico, 25 March 2020)

Governments are trying to leverage mobile technology in tracking and controlling the spread of the virus.[5] Mobile telephone carriers are asked to submit information[6] and Google has volunteered tracking information. [7] Different app solutions have been deployed or

[1] EU vs Disinfo: Coronavirus in Russia: Independent Journalists call the bluff.
[2] Graphika: Iran's IUVM turns to coronavirus.
[3] *The Sun*: Bizarre '5G caused coronavirus' conspiracy theory that spread on YouTube is still going viral on WhatsApp.
[4] *The Guardian*: Broadband engineers threatened due to 5G coronavirus conspiracies.
[5] Politico: In fight against coronavirus, governments embrace surveillance.
[6] Politico: Commission tells carriers to hand over mobile data in coronavirus fight.
[7] *The Wall Street Journal*: Google offers user location data to health officials tackling coronavirus, France24: Google to publish user location data to help govts tackle virus

are planned for contact tracing, quarantine control or tracking symptoms. Poland, for example, has deployed a quarantine checking app[8] and is reported to be developing an app for contact tracing;[9] and Google and Apple are creating APIs to enable tracing contacts between people.[10]

For military organisations in particular, this may, in addition to the privacy issue for the individuals, risk the tracking of sensitive personnel and operations. The solution being developed by Google and Apple uses a scheme with changing identifiers and no geo-positioning, which looks as if it will not make it possible to track or identify a phone.[11] But privacy and security concerns have been raised about the solutions already in place, for example in the UK.[12]

Increased government cyber-enabled authority in a time of crisis needs to be monitored. The tools can have benefits when tracking the spread of the virus, and give valuable information for prognosis and prevention. At the same time, they have the potential to be misused in the name of public safety, and if the data is not properly secured, there is the possibility of an adversary tracking logistic movements or troops. The general deployment of these tools, their use by the military, and the use of mobile devices, in general, have to be a careful trade-off between risks and benefits.

Working remotely is here to stay and requires a new focus on personal cyber hygiene

'A new emphasis on telework at the Defense Department in response to the COVID-19 pandemic could change work culture at the Pentagon, officials said'. (FCW, 14 April 2020)

The COVID-19 pandemic has caused almost all organisations, including the military, to work in new ways. This makes them more vulnerable[13] to some types of cyber threats,[14] not least because of a large number of laptop computers being more exposed to threats from the internet.[15]

Parts of this new way of working will probably be here to stay. Remote working will become a more natural mode of working in the post-COVID-19 world. From a crisis preparedness point of view, this is good. Having the tools for remote working in place, the staff trained and used to working with them, and the relevant policies and procedures approved and implemented will ease the transition when the need arises. If managed correctly, the ability to work remotely will be an important part of ensuring business continuity.[16]

The challenge is to build and maintain adequate security. Tools that may have been deployed quickly in response to the current crisis need to be assessed and then continuously monitored and improved. Developing solutions that can be securely deployed at home, without requiring a large cyber workforce, is important. It is also important to start building a solid security culture.[17, 18] The work-from-home scenario puts even more emphasis on the individual's responsibility for maintaining security.

Militaries need to stress cyber hygiene at home, and train employees in what this means. Many non-military solutions have been put to use to maintain continuity of operations. Poor cyber hygiene at home and lack of security training for the new tools lead to vulnerabilities that can be exploited.

---

[8] Politico: Poland's coronavirus app offers playbook for other governments.
[9] Reuters: Poland works on smartphone app to help stop coronavirus outbreak.
[10] Apple: Apple and Google partner on COVID-19 contact tracing technology.
[11] TechCrunch: Apple and Google update joint coronavirus tracing tech to improve user privacy and developer flexibility.
[12] TechCrunch: UK privacy and security experts warn over coronavirus app mission creep.
[13] *The Sydney Morning Herald*: 'Absolute perfect time' for cyber criminals to attack, as businesses work from home'.
[14] Infosecurity Magazine: Working from home during #COVID19: increasing threats.
[15] Help Net Security: Surge in remote working reveals concerns around unprotected endpoints.
[16] DarkReading: Getting ready for the next business continuity challenge.
[17] Help Net Security: Cybersecurity in a remote workplace: A joint effort.
[18] DarkReading: Why all employees are responsible for company cybersecurity.

2. Targeted threats against the military and national security

Disinformation targeting military personnel aims to undermine unity in NATO

'A Polish government official says Poland has been hit by a "complex disinformation operation" that appears aimed at weakening the Polish-US alliance and is consistent with previous Russian cyberattacks'. (*The New York Times*, 25 April 2020)

The campaign used a fake letter from the Rector of the War Studies Institute in Warsaw to call on students to oppose the 'American occupation'. The theme of this attempt fits in with the wave of COVID-19-related disinformation in that it tries to push a wedge between the US and its allies.

3. Other cyber activities relevant to the military

Securing video conferences isn't just about excluding certain providers

'But security researchers have called Zoom "a privacy disaster" and "fundamentally corrupt" as allegations of the company mishandling user data snowball'. (*The Guardian*, 2 April 2020)

As we all know, the COVID-19 pandemic has caused massive changes in how and where we work. Meetings are no longer held in person, and we rely heavily on video conferencing instead.

The fast, global spread of the virus has caused militaries to implement ad hoc solutions to conduct business as they have been forced to work remotely. Many did not have technology, processes and procedures in place to handle working from a remote location in peace-time. This lack of policy resulted in confusion and wasted time, and affected military readiness as tasks were postponed or ignored.

Lately, there have been many discussions and investigations on the security of teleconferencing solutions, with the major focus on the Zoom platform.[19] Yet the possibility remains that its competitors may be carrying similar security flaws and vulnerabilities. Zoom has been working on solving the security issues by, for example, releasing an updated version of the application,[20] and other remedies, but the recommendations are to be careful. The interest in the security of Zoom has attracted bug bounty hunters and actors selling vulnerabilities on the grey market.[21]

In addition to the misleading security claims from Zoom and several vulnerabilities in the service itself,[22] malicious actors are pushing Trojans in the form of fake Zoom applications.[23]

Many government agencies around the world, including the FBI,[24] have published warnings about the vulnerabilities and risks of the Zoom platform. Although Zoom seems to be taking the reports seriously and has been working to patch those vulnerabilities,[25] many users are leaving the platform,[26] at least for conferences with sensitive content.

It is important, however, to remember that the focus on vulnerabilities in Zoom does not mean that other products are free from vulnerabilities. Another example was a vulnerability, now fixed, in Microsoft Teams.[27]

For the military, using vulnerable video conferencing applications means a risk of leaking sensitive information, which in turn could jeopardise operations or give information to malicious actors involved in disinformation campaigns.

This calls for a serious assessment of the tools used for conferencing and selecting the right tool whenever sensitive or classified information is to be communicated. Since many solutions, like Zoom, do not encrypt

[19] Motherboard, Tech by Vice: Interest in Zoom zero-day hacks is 'sky-high' as meetings move online.
[20] Zoom: Zoom hits milestone on 90-Day security plan, releases zoom 5.0.
[21] *Vice*: Hackers are selling a critical Zoom zero-day exploit for $500,000.
[22] Citizen Lab: Move fast and roll your own crypto.
[23] SecurityWeek: Trojanized Zoom apps target remote workers.
[24] FCW: FBI warns on Zoom conference security.
[25] Bank Info Security: Zoom rushes patches for zero-day vulnerabilities.
[26] Help Net Security: Will Zoom manage to retain security-conscious customers?
[27] ThreatPost: How patched flaw allowed attacker to take over an organization's entire roster of Microsoft Teams accounts.

video and audio streams from end-to-end, it is important to be able to trust the interconnection point, where the data will be decrypted and re-encrypted. For the most sensitive conversations, it would be wise to have this point on-premises.

The market for zero-days provides the means to build a cyber-arsenal without having to hire the talent

'Zero-day [vulnerabilities] are increasingly likely to be bought and sold by malware vendors targeting the Middle East with their dodgy wares, according to FireEye. "While not every instance of zero-day exploitation can be attributed to a tracked group, we noted that a wider range of tracked actors appear to have gained access to these capabilities," said the threat intel group in a blog post published today'. (The Register, 6 April 2020)

Increased trade in zero-days [28] means that well-funded actors may acquire better tools[29] without needing to build the capability to find these themselves. A well-developed and lucrative market for vulnerabilities may also lure independent vulnerability researchers away from vendors' bug bounty programmes. This may mean more malicious actors with access to exploitable vulnerabilities, and therefore a bigger threat against otherwise well-protected networks.

As military users rely more and more on commercial off-the-shelf products, they risk becoming vulnerable to flaws in products that are heavily researched and where vulnerabilities and exploits are being traded in this way.

This highlights the need for protection against unknown vulnerabilities. Protection against this type of threat can never rely on just one type of security measure. The overall strategy should be to build robust security architectures, adhering to the defence-in-depth principle and air-gapping systems or connecting through military-grade cryptosystems where appropriate.

For systems that need to be connected to the internet or other public networks, security products based on detection of anomalies should be considered. Key actors supporting initiatives for responsible disclosure of vulnerabilities may also gain more importance in the longer term. Google has, for example, created a rewards programme to encourage 'white hat' bug hunters.[30]

Lack of mitigating measures from ISPs make hijacking of internet traffic possible

'Earlier this week, traffic meant for more than 200 of the world's largest content delivery networks (CDNs) and cloud hosting providers was suspiciously redirected through Rostelecom, Russia's state-owned tele-communications provider. The incident affected more than 8,800 internet traffic routes from 200+ networks, and lasted for about an hour'. (ZDNet, 5 April 2020)

The incident was what is known as a BGP[31] hijack, where incorrect routing information is spread causing traffic to be sent in the wrong direction.[32] These incidents show that internet routing is not as stable and secure as one would hope and that malicious actors can manipulate the system.

The weakness makes it possible to eavesdrop on internet traffic, direct traffic to fake webservers, [33] or make a denial of service attack by having traffic routed to a dead-end. This risks must be taken into consideration when relying on the internet as a communications channel.

The eavesdropping and false server issues can be mitigated by the use of robust authentication of the other party and end-to-end encryption that protects against man-in-the-middle attacks. As has been shown by the Zoom case, trusting a vendor's claims of end-

[28] Bank Info Security: More zero-day exploits for sale: Report.
[29] FireEye: Zero-day exploitation increasingly demonstrates access to money, rather than skill.
[30] Security Week: Google creates COVID-19 grant fund to boost bug hunting Google security blog: Research grants to support Google VRP bug hunters during COVID-19.
[31] The Border Gateway Protocol (BGP) specifies how routers between parts of the internet (called autonomous systems) exchange information on how to route traffic a specific destinations.
[32] BGP hijacking is possible because the system relies on autonomous systems trusting the routes that are shared with them.
[33] Cyware Social: Why BGP hijacking remains a security scourge for organizations worldwide.

to-end encryption may not be enough. Encryption is hard to get right, and the architecture and implementation of such solutions need to be evaluated carefully by trusted parties to assess the security posture.

Protecting against major network outages because of misrouted traffic is more difficult for individual actors. These problems need to be mitigated by having robust alternative communication paths.

A long-term solution will require the BGP protocol to evolve to be more secure, something that has proven to be difficult and will take a long time to implement. In the meantime, major network providers need to implement such mitigating measures and best practices as have been developed. [34] Initiatives to further develop and promote the security of internet routing must be supported.

Cyber attacks against the health care sector continue

'The Czech Republic warned international allies on Thursday of an imminent wave of disruptive cyberattacks against the country's hospitals and other parts of its critical infrastructure'. (Reuters, 17 April 2020)

The Czech Republic has warned of imminent attacks on particular healthcare facilities[35] and unsuccessful attacks have been reported. [36] The attacks may affect availability, confidentiality and integrity of information. International reaction to the warning includes the US voicing its support for the Czech Republic [37] and Estonia condemning the attacks.[38]

The expected attacks are not isolated. The warning should be seen in the light of other targeted attacks, such as those against research facilities involved in work related to COVID-19[39] and the WHO.[40] Google has also warned that nation-backed hackers are targeting healthcare organisations.[41]

If civilian healthcare is attacked, the care of military personnel will suffer and the need for the military to support the health care sector will increase.

Such state-sponsored attacks are clearly not in line with the cyber norms promoted by NATO nations and others. To deter such attacks, and provide a foundation for an active response, attribution by many Allies is important.

State-sponsored attack against specific users of a commercial email provider

'State-sponsored hackers have used a zero-day vulnerability to hijack a small number of high-profile email accounts at Estonian email provider Mail.ee. The attacks took place last year and the vulnerability in Mail.ee's service has been fixed, the Estonian Internal Security Service (KaPo) said in an end-of-year report published this month'. (ZDNet, 29 April 2020)

According to the report, attackers were able to compromise several targeted email accounts and have mail forwarded from those accounts. In the report, the Estonian Internal Security Service (KaPo) makes a number of recommendations related to choosing an email provider:[42] If possible, avoid using an external email provider for the most sensitive information and do not use unencrypted email for sensitive communications. It is also important to train personnel not to use private email accounts for work purposes.

4. Policy and strategy developments

The Cyberspace Solarium Commission underlines the importance of cyber security during the COVID-19 pandemic

'Cyberspace Solarium Commission staffers have sent the commissioners an additional section for its report focused on how the

[34] Wired: You can now check if your ISP uses basic security measures.
[35] National Cyber and Information Security Agency (NUKIB): Warning.
[36] Intellinews: Czech healthcare sector under serious cyber attack.
[37] U.S. Department of State: The United States concerned by threat of cyber attack against the Czech Republic's healthcare sector.
[38] ERR: Reinsalu condemns cyber attacks against Czech critical infrastructure.
[39] Bank Info Security: FBI: Hackers targeting US COVID-19 research facilities.
[40] Reuters: Hackers linked to Iran target WHO staff emails during coronavirus - sources.
[41] Nation-backed hackers tune attacks to COVID-19 fears: Google.
[42] KaPo: Annual Review 2019

coronavirus underscores the importance of the group's work, according to two staffers and two other people familiar with the matter'. (Politico, 29 April 2020)

The proposed annex to the Solarium Commission's report is both pointing out what recommendations are most important in the current situation and adding areas of cyber security that have come to light but were not covered by the original report. If the commissioners decide to incorporate the annex in the report it will be one more indication that the pandemic has become a wake-up call, not just for the health sector, but also very much for cyber security and digital business continuity planning.

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