CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Recent Cyber Events and Possible Implications for Armed Forces

#4 – July 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

Leaked government data could put personnel at risk

'It was reported on Friday (May 29) that a government database of more than 20 million Taiwanese citizens was leaked on the dark web. […] It is unusual for an entire nation's database to be leaked, [the cyber threat intelligence company] Cyble reported.' (Taiwan News, 30 May 2020)

The leak of the Taiwanese home registry database is an unusually large breach. The leaked data is said to include names, addresses, genders, dates of birth and other private information of citizens. Data breaches of various sizes have become a more common tactic of hostile actors. Well-known cases include the 2012 breach of outsourced Swedish government databases, including information about police employees and the addresses of people with protected identities; a similar case in Denmark;[1] and the US Office of Personnel Management breach, which included sensitive information on government employees.[2]

Even less sensitive information may aid foreign intelligence services in identifying and targeting individuals in sensitive positions. Leaks of individual records or pieces of information are usually not so damaging, but a complete database could be a much more useful source for an adversary's intelligence service as information can be combined and compared in different ways. Detailed knowledge about individuals gained from such leaks could, for example, aid in making credible phishing campaigns or preparing convincing documents containing malware. The more personal information an adversary has, the more likely those types of attacks are to be successful.

Management and protection of population and property registers are usually not under the direct control of national security or military authorities, which calls for interagency cooperation and careful risk analysis in determining and implementing the appropriate security measures and controlling what information can be held in the registers.

2. Other cyber activities relevant to the military

Australia's response to disinformation campaigns

'The Australian government recently announced plans to establish the country's first taskforce devoted to fighting disinformation campaigns, under the

[1] Newsweek: Pirate Bay co-founder found guilty of hacking crimes in 'historic' case

[2] Wired: Inside the cyberattack that shocked the US government

Department of Foreign Affairs and Trade (DFAT).' (The Conversation, 23 July 2020)

The act of organised, systematic and often covert distribution of false information by groups or individuals to influence public discourses and opinion is known as a disinformation campaign. The COVID-19 pandemic showed a spike of news reports about disinformation operations through social media, potentially by state actors.[3]

The pandemic does not seem to be the only public discourse targeted by disinformation operations, as news articles have recently surfaced claiming that the protests in the USA are subject to false rumours and doctored images. Examples mentioned by the press include a screenshot of a TV-show featuring a big explosion next to the Washington Monument, rumours about a police officer disguised as a CNN reporter and claims that mobile phone communication was blocked to prevent reports of violent police behaviour.[4] It was also reported that white nationalist groups posed as members of Antifa to tweet calls for violence.[5]

Social media platforms including Twitter, Facebook, LinkedIn, Reddit and YouTube issued a joint industry statement claiming to be working together to combat fraud and misinformation about COVID-19. [6] Yet the automated algorithms used to discover, label and remove misinformation do not seem to work quickly enough to stop the spread and do not always seem to detect edited re-uploads.[7]

Concerning COVID-19 and misinformation, Australian foreign minister Marise Payne said during a recent speech: 'For our part, it is troubling that some countries are using the pandemic to undermine liberal democracy to promote their own more authoritarian models,' [8] reportedly noting a report by the European Commission about foreign actors and countries carrying out disinformation campaigns.[9]

The Australian government now plans to establish a national taskforce to fight disinformation campaigns under its Department of Foreign Affairs and Trade.[10] Disinformation operations in cyberspace and social media can have a considerable reach and have the potential to alter public perceptions and undermine democracy.

Australia's response to disinformation campaigns might have some global consequences for misinformation in cyberspace and while there is not yet much information about the taskforce that is to be established, it might be interesting to follow the development to evaluate its impact.

Protection against cyber threats is essential for industrial control systems

'Multiple decades of research have focused on building more secure and resilient systems by incorporating defensive techniques into computer systems. […] However, many cyber-physical systems (CPS) and safety-critical application domains such as industrial control systems (ICS), avionics, automotive and other mission-critical applications have not seen the widespread adoption of many of these generally effective software defences.' (AFCEA SIGNAL: June 1 2020)

Cyber-physical systems (CPS) play an important role in military operations, both as parts of specific military systems such as avionics and weapons applications and as parts of critical infrastructure underpinning military operations. This is evident in the domain of military mobility, where there is a dependence on ports, railways and electricity providers, all of which rely heavily on cyber-physical systems.

Attacks against CPS may have almost direct effects in the physical world and may result in the inability to perform operations or even physical harm or loss of life. The cyber risks of these systems are therefore different from the ones associated with most traditional IT-

[3] EU vs. Disinfo: EEAS special report update: short assessment of narratives and disinformation around the COVID-19 pandemic
[4] NPR: False rumours and doctored images went viral during the D.C. protests
[5] NBC News: White nationalist group posing as antifa called for violence on Twitter
[6] Facebook: Working with industry partners
[7] Forbes: COVID-19 misinformation remains difficult to stop on social media
[8] *South China Morning Post*: Coronavirus: Australia's Foreign Minister Marise Payne says China is spreading 'disinformation'
[9] *The Sydney Morning Herald*: Foreign Minister Marise Payne hits out at Chinese, Russian 'disinformation'
[10] The Conversation: China's disinformation threat is real. We need better defences against state-based cyber campaigns

systems. Whereas safety aspects have often been a priority in CPS, security against adversary attacks by cyber means have often not been looked at as rigorously.

In the article quoted above, some of the commonalities and differences between the two domains and some of the possible security measures and the evaluation by scientists at MIT's Lincoln Laboratory are described. It is clear that the type of cybersecurity measures now commonly implemented for enterprise computing environments have to be brought more consistently to CPSs and operational technology (OT), but the technology has to be adapted and evaluated for the new domain and the real-time requirements that are common there.

One interesting development in cybersecurity for ICS is the application of artificial intelligence (AI) to the problem. Siemens recently announced a collaboration with machine learning company SparkCognition in this field. [11] The AI-driven cybersecurity system is targeted at the energy sector and will monitor and detect cyberattacks against endpoints and remote OT assets. Leveraging AI may give this type of solution improved capabilities to detect zero-day threats compared to conventional anti-virus.

Following up on Zoom's security, privacy and involvement with China

'For most users in most situations, Zoom's current security seems adequate. Given the service's rapid proliferation, though, including into high-sensitivity settings like government and health care, it's important that the company give a real explanation of what encryption protections it does and doesn't offer.' (Wired, 3 April 2020)

The cloud platform software Zoom remains a topic of many news reports since COVID-19 introduced a heightened demand for easy-to-use video-teleconferencing tools. While the US-based company behind the software, Zoom Video Communications, is being traded at a record high, [12] some have voiced their concerns about its increased use and the software itself. Covered in the May issue of this publication were the concerns of security researchers about the company's handling of privacy. [13] Related to these issues, Zoom's encryption was investigated by Citizen Lab and its opaque key generation and centralised key management system was addressed. A discrepancy seems to exist between the claims made by the company and investigative results.[14]

A more recent development is Zoom's confirmation that meetings were blocked and accounts of US-based Chinese activists were closed following a request by the Chinese government. [15] Allegedly, the reasoning behind Zoom closing meetings commemorating the 31st anniversary of the Tiananmen Square massacre was compliance with local law – a polarising statement given that the activists were reportedly in the US.[16]

While Zoom has its headquarters in the US, the app itself is reported to have been developed in China by three companies, two of them owned by Zoom. Citizen Lab voices a suspicion that encryption keys might be distributed through servers located in China, which could potentially be concerning since Zoom may have a legal obligation to disclose these keys to Chinese authorities.[17]

A driving factor behind Zoom's popularity may be ease of access, because it is quasi platform-agnostic and thus barrier-free for users. The possibility to use a web client allows users to circumvent limitations of software solutions often used by armed forces, which are typically restrictive and usually on-premises rather than in the cloud. Although such restrictions are limiting, they are put in place as security or privacy measures. Zoom shows that ease of use can enable widespread and fast adoption of technology by the military as a means of command and control during extreme circumstances.

---

[11] PR Newswire: SparkCognition and Siemens to Deliver New AI-driven Cyber Defense System for Endpoint Energy Assets
[12] CNBC: Zoom tops Lyft as the most valuable tech IPO of the year so far
[13] The Guardian: 'Zoom is malware': why experts worry about the video conferencing platform
[14] Wired: So wait, how encrypted are Zoom meetings really?
[15] SecurityWeek: U.S. Officials 'Alarmed' by Zoom Cooperation With China
[16] Axios: Zoom closed account of U.S.-based Chinese activist 'to comply with local law'
[17] The Citizen Lab: Move fast and roll your own crypto

The rise of cloud-based video conferencing solutions like Zoom introduces the requirement for an infosec examination determining if certain risks, like the development of applications and hosting of services in potentially adversarial nations, are acceptable. The most pragmatic approach for using cloud-based video conferencing tools may be to be conscious of the sensitivity of topics and residual information and not to address anything classified.

Issues about privacy, encryption, state cooperation and affiliation and legal obligations emerging from the discourse surrounding Zoom can be regarded as indicators for requirements and new best practices when futureproofing teleworking. Reacting to the massive rise of Zoom, many competitors have advertised the same advantages without the criticised downsides while focusing on privacy and encryption and incentivising users to re-evaluate their choice. Correspondingly, Zoom introduced a 90-day plan to address and improve privacy and security including end-to-end encryption for group calls.[18]

The two-edged sword of open-source software

'Open source software (OSS) has quickly transformed both how modern applications are built and the underlying code they rely on. Access to high-quality and powerful open source software projects has allowed developers to quickly integrate new capabilities into their applications without having to reinvent the wheel. […] However the open source revolution also comes with its own potential pitfalls. […] . In short, while open source projects can rapidly go viral, so can their vulnerabilities.' (RiskSense Spotlight Report, May 2020)

Open source is a term used to describe software and other products that are released under a licence which grants permission to use, modify and distribute its source code. According to a study conducted by Red Hat, 95% of organisations regard open-source software as an important strategic element of their business.[19]

Armed forces are no exception when it comes to using open-source software or open-source software components; the German armed forces, for example, are testing the open-source distributed communications platform Matrix. [20] The threat intelligence platform MISP, which is not only used in the private sector but also by NATO and many national and military CSIRTs, is open-source software.

Recent reports show an alarmingly high number of vulnerabilities found in open-source projects, a number that has doubled since the previous year, with the Jenkins automation server and MySQL at the top of the list by reported vulnerabilities. [21] The report also states that it took an average of 54 days to report these vulnerabilities, which gives a big window of opportunities for malicious actors.

While open-source software has considerable advantages like access to the source code and the ability to modify it to fit unique needs, it comes with its downsides. Since popular open-source projects are very common, any vulnerabilities will be widespread and therefore attractive attack vectors for malicious actors. The upside of using popular open-source software is the chance for quick detection and patching of vulnerabilities increases with the size of the community.

Budget cuts may affect compliance with cybersecurity rules

'Cybersecurity incidents at NASA rose by 366% last year, according to data collected by virtual network provider AtlasVPN. From a total of 315 in 2018, they rose to 1,469 in 2019, at a time when NASA's cybersecurity budget declined by $3.1 million over the same period.' (In Cyberdefense, 9 June 2020)

Being in the spotlight among other governmental agencies, NASA saw an increase in cybersecurity incidents of 366% last year, compared to the previous one, while the agency's cybersecurity budget declined by $3.1 million.

[18] Lexology: Are we (finally) ready to Zoom?
[19] Red Hat: The state of enterprise open source
[20] GFOSS: German armed forces testing open source chat
[21] SecurityWeek: Nearly 1,000 vulnerabilities found in popular open source projects in 2019

Governmental agencies with other critical infrastructure companies usually suffer the biggest and continuous cyberattacks. Although there are many other factors also at play, the correlation between cybersecurity budget cuts and the increased effects from cyberattacks requires the attention of governments regarding the severity of possible consequences of a reduced cybersecurity posture.

Cybersecurity and security awareness training are among the things that are at risk when cybersecurity budgets are cut. NASA's cyber-incident data indicates that many of the incidents were related to improper use. This shows that continuing user training is important for the security posture of an organisation.

3. Policy and strategy developments

Dedicated Cyber Units to support military operations

'The British military has launched its first dedicated cyber regiment for use against hostile states and terrorist groups at home and abroad, the Ministry of Defence has announced. The 13th Signal Regiment, drawing personnel from across the forces, will be used to carry out offensive cyberspace operations as well as counter hacking and propaganda from adversaries.' (Independent, 4 June 2020)

In addition to the new UK cyber regiment, the US Army created the 915th Cyber Warfare Support Battalion to integrate intelligence, cyber, electronic warfare, signals, information operations and fires into one formation, while also being able to deliver effects remotely and through local expeditionary cyber teams that will plug into the cyber and electromagnetic activities (CEMA) sections located in each brigade planning cell.[22]

First sanctioning using EU's Cyber Diplomacy Toolbox?

'The European Union is getting ready to slap sanctions on a group of Russian hackers, according to three diplomats involved — a move that would mark a turning point in the bloc's efforts to address foreign hacking. The sanctions, expected later this year, come after the German government announced it "had evidence" tying members of a Russian hacking group to the cyberattack on the Bundestag in 2015.' (POLITICO, 3 June 2020)

The discussion of sanctions follows the arrest warrant issued for a Russian individual earlier this year and comes almost five years after the original incident. [23] Russia is denying the allegations, claiming that there is no evidence of its involvement.[24] This could be the first use of use of sanctions as part of the Cyber Diplomacy Toolbox.[25] The toolbox allows for sanctions, such as freezing funds, against persons, entities and bodies involved in a cyberattack threatening the EU or its Member States.

The effect of sanctions so long after the event may be questionable, but the EU coming together like this will aid the development and increased observance of norms of responsible state behaviour in the cyber domain. EU Commission President Ursula von der Leyen also recently suggested that China has been behind cyberattacks against hospitals in Europe and declared that such attacks cannot be tolerated.[26]

A united front against unacceptable behaviour in cyberspace will, of course, have a better chance of being effective than nations responding individually. Holding an entity or body supporting an attack responsible could also be a bolder step than charging only the individual that actually carried out the attack.

We have yet to see if this case will result in sanctions; some comments indicate that this is far from certain. [27] The fact that the attacks are characterised as political espionage rather than a destructive attack may make it less likely that sanctions will be put in place. The effect could also be limited due to the fact that

[22] Fifth Domain: How the Army is taking cyber units to the battlefield
[23] ZDNet: German authorities charge Russian hacker for 2015 Bundestag hack
[24] SecurityWeek: Russia Angrily Denies German Allegations on 2015 Cyberattack
[25] NATO CCDCOE INCYDER: European Union establishes a sanction regime for cyber-attacks
[26] EURACTIV: Von der Leyen: Chinese cyberattacks on EU hospitals 'can't be tolerated'
[27] Lawfare: The Case Against EU Cyber Sanctions for the Bundestag Hack

the sanctions would not imply attribution of the attacks to any state or government. It also remains to be seen if the EU will be able to speed up the process in future cases, but there is some promise of a unified European response that will put a price tag on this type of cyberattack and act to deter future attacks.

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