CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Recent Cyber Events and Possible Implications for Armed Forces

#7 – November 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

Cyber conflict in Nagorno-Karabakh

'It's the worst outbreak of violence related to Nagorno-Karabakh since Armenia and Azerbaijan, two former Soviet republics, fought a war over the enclave in the 1990s. And this time, hacking has come with the fighting.' (CyberScoop, 6 October 2020)

Tensions over the territory of Nagorno-Karabakh are decades old. Recently the situation has flared up into violent conflict. As is commonplace in the modern era, spillover to cyberattacks and information campaigns from both sides accompany kinetic action. In most cases, it is related to defacing internet pages and supporting information operations.[1] Attacks targeted public and private institutions in the energy industry. [2]

Sophisticated cyberattacks have been employed in this conflict. One example is PoetRAT malware which targets government and critical infrastructure sectors. According to Cisco Talos, actors have modified PoetRAT malware, showing increased capacity and maturity. PoetRAT was reportedly used against Azerbaijan previously and continue during the current campaign. New versions of PoetRAT are said to target the Azerbaijani public sector by using malicious Microsoft Word documents. [3] This allows targeting through spear-phishing specific individuals to collect intelligence. Overall, the campaigns using PoetRAT seem to be efficient and to have given the cyber actors access to sensitive information.

What it means:

1. Cyber operations are part and parcel of kinetic military campaigns. Their tactical use is still in its infancy, while its use for strategic and operational objectives is real and promising.
2. If proper tools for malicious activity are employed, it will be easier and quicker to use them within military campaigns. It also shows that a cyber campaign could be employed quicker and more efficiently to produce an effect.
3. Recoding of malware is constant and follows the KISS principle – 'keep it simple, stupid'. A campaign requires a thorough analysis of the target and an understanding of the cognitive domain to influence specified targets.

[1] BBC: Nagorno-Karabakh: The Armenian-Azeri 'information wars'
[2] Cisco Talos Blog: PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors
[3] Cisco Talos Blog: PoetRAT: Malware targeting public and private sector in Azerbaijan evolves

US charges Russian military hackers with attacking American companies, targeting foreign elections

'The FBI has repeatedly warned that Russia is a highly capable cyber adversary, and the information revealed in this indictment illustrates how pervasive and destructive Russia's cyber activities truly are […] But this indictment also highlights the FBI's capabilities. We have the tools to investigate these malicious malware attacks, identify the perpetrators, and then impose risks and consequences on them. As demonstrated today, we will relentlessly pursue those who threaten the United States and its citizens.' FBI Deputy Director David Bowdich (US Department of Justice, 19 October 2020)

The US Justice Department has indicted six Russian military intelligence officers from the Russian Main Intelligence Directorate, known as the GRU, for malicious cyber activity. The individuals have been judged to be members of 'Sandworm' the GRU unit that was behind attacks on Ukrainian infrastructure, widespread ransomware campaigns, and a series of attacks on the 2018 Winter Olympics, with the intention to sabotage the running of the event. The attacks leveraged 'some of the world's most destructive malware', including Killdisk and Industroyer (responsible for the Ukrainian blackouts), NotPetya (thought to have caused almost $1bn in damage to three victims named in the indictment) and Olympic Destroyer, a destructive malware attack against the opening ceremony.

The US's allies have expressed support for the US indictment, calling it 'a step towards a more stable cyberspace'. [4] In a separate announcement on 19 October, the UK National Cyber Security Centre also confirmed that the GRU was responsible for the Winter Olympics cyberattacks.[5]

EU imposes sanctions on Russian military intelligence actors over 2015 Bundestag cyberattacks

'The Council today imposed restrictive measures on two individuals and one body that were responsible for or took part in the cyber-attack on the German Federal Parliament (Deutscher Bundestag) in April and May 2015. This cyber-attack targeted the parliament's information system and affected its ability to operate for several days. […] A significant amount of data was stolen and the email accounts of several members of parliament, including that of Chancellor Angela Merkel, were affected. (EU Council press release, 22 October 2020)

This is the second time the 'restrictive measures' of the EU Cyber Diplomacy Toolbox (EU's Framework for a Joint Diplomatic Response to Malicious Cyber-Activities) have been applied. The sanctions consist of travel bans and asset freezes against the head of the GRU, Igor Kostykov, Dmitry Badin, a military intelligence officer, and the GRU's 85th Special Centre for Military Services. EU individuals are prohibited from making funds available to them.[6] There are now six GRU officials on the EU sanctions list over cyberattacks.[7]

The Cyber Diplomacy Toolbox adopted in 2017 and subsequently revised in 2019, enables the EU to impose targeted restrictive measures to deter and respond to those cyberattacks which constitute an external threat to the EU or its member states, including cyberattacks against third countries or international organisations.

The Trickbot botnet recovers after disruption by US Cyber Command

'The US Cyber Command, the Defense Department division in charge of its cyberspace operations, recently mounted an operation to disrupt one of the most massive and notorious botnets today. According to The Washington Post, CyberCom successfully (albeit temporarily) interrupted the Trickbot botnet's operations at least a couple of times over the last few weeks. ' (Engaged October 10th, 2020)

Trickbot is malware described as a banking Trojan mainly targeting Windows computers. According to Malwarebytes, it targets international banks and is designed with modules, each having specific jobs such as to steal bitcoin wallets, harvest emails and

[4] Estonian MFA (@MFAestonia) via Twitter
[5] GOV.UK: UK exposes series of Russian cyber attacks against Olympic and Paralympic Games
[6] Official Journal of the European Union, L 351I
[7] CCDCOE: Si vis cyber pacem, para sanctiones: the EU Cyber Diplomacy Toolbox in action

credentials, encryption, and command and control, essentially turning infected machines into bots.[8]

At the beginning of the month, it was reported that US Cyber Command managed to temporarily disrupt Trickbot's operations by sending a command to infected machines to disconnect. While the disruption was successful, no permanent harm to the network was caused and the botnet became operational again.[9]

The end of the month was marked by a warning from the FBI and other US government actors concerning a ransomware threat to US hospitals and healthcare providers. According to reports, the US health care systems are under threat by Trickbot and the government warned endangered entities to perform backups and to disconnect non-essential systems. [10] The latest wave of ransomware attacks infected 24 health care institutions with no signs of a slowdown. Independent efforts by US Cyber Command, Microsoft and others to put a stop to Trickbot did not seem to be effective enough to dissolve the botnet.[11]

These recent events show not only the resilience of botnets in face of major players but also how botnet capabilities could be used to attack military systems in the same, seemingly well-coordinated fashion as hospitals. On the policy side, international cooperation needs to be fostered so that criminal activity in the ransomware sector can be combatted more effectively across national borders.

2. Other cyber activities relevant to the military

Physical security threatened when blueprints are leaked

'Details of bank vault floor plans, alarm systems and the security arrangements for Swedish authorities have been leaked online after a security company was hacked, local media reported Tuesday.' (SecurityWeek, 27 October 2020)

The security company Gunnebo seems to have been hit by an attack from a ransomware gang. Vast amounts of data were exfiltrated and a substantial amount leaked on the dark web, including blueprints of buildings belonging to customers like banks and the Swedish tax agency. From reports, it seems like no classified information was leaked, but some documents are said to have had official confidentiality markings.[12] It is not clear what security agreements were in place between the company and its customers. From comments on the leaked documents in news reports it is, however, clear that they contain information on security arrangements that may give someone an advantage in planning a physical intrusion into the building.

Although the object of the attack was probably to extort money rather than steal the sensitive blueprints, the stolen and leaked documents may very well end up in the hands of criminals and foreign intelligence agencies, so the damage is done. Paying the ransom, something Gunnebo is reported as saying that it will not do, is no guarantee that the information will not be sold to others.[13] Giving highly sensitive information like this to contractors may be unavoidable, but when doing so several things should be kept in mind as adversaries will seek out and seek to obtain the information they want wherever it is least tightly protected:

- Make sure only what needs to be shared is given away, creating less sensitive digests or selections of information if needed;
- Mark sensitive information clearly so that is possible to see what level of protection it needs;
- Make detailed agreements with contractors on how your information should be protected; and
- Monitor and audit the contractor's management of your information, including cybersecurity measures.

[8] Malwarebytes Labs: Trojan.TrickBot
[9] Engadget: US Cyber Command disrupted the notorious Trickbot botnet
[10] ZDNet: FBI warning: Trickbot and ransomware attackers plan big hit on US hospitals
[11] Wired: Ransomware hits dozens of hospitals in an unprecedented wave

[12] HackRead: Mount Locker ransomware group leaks 18Gb worth Gunnebo AB data, *Dagens Nyheter*: Enorm säkerhetsläcka – hemliga uppgifter om riksdagen och banker ute på nätet
[13] Teller Report: DN: Huge hacking case in Sweden - hackers steal information about corporate, banking and parliamentary security systems

World leaders targeted in an attempted phishing attack

'The Phosphorous APT has launched successful attacks against world leaders who are attending the Munich Security Conference and the Think 20 (T20) Summit in Saudi Arabia, Microsoft warns.' (Threatpost, 28 October 2020)

It has been proven once again how vulnerable we are in the time of COVID-19, since almost all regular work has moved from the physical to the virtual sphere. This time, a cybersecurity incident occurred pertaining to both the Munich Security Conference and the T20 Summit in Saudi Arabia. Both conferences have been scheduled as virtual due to the COVID-19 situation.

Microsoft had detected and stopped APT35, a hacking group with ties to Iran. The hacking group used fake invitations sent by email to target over 100 high-profile individuals by masquerading as the conference organiser using email addresses such as munichconference@outlook.de and t20-saudiarabia@outlook.sa. The goal of the perpetrators was to redirect invitees to the fake websites posing as official domains for the conference to gain their credentials. According to Microsoft, the attackers' goal was to gather intelligence as they obtained credentials to log into the victim's inbox and access sensitive information.

In this time of pandemic, this should be an additional warning to governments and NATO, as most politicians, diplomats and civil servants are working from home. We must all be aware that technical solutions alone are insufficient to eliminate vulnerabilities and threats. In addition to appropriate technical solutions, business continuity must also be ensured, along with an appropriate level of awareness of the threats and the maintenance of a strong cybersecurity culture.

3. Policy and strategy developments

US releases new critical technology and data strategies

'The DoD now recognizes that data is a strategic asset that must be operationalized in order to provide a lethal and effective Joint Force that, combined with our network of allies and partners, sustains American influence and advances shared security and prosperity.' (US Department of Defense, 30 September 2020)

The data strategy highlights initial areas of focus as (1) all-domain operations; (2) senior leader decision support; and (3) business analytics. The stated aspirations of the data strategy are to facilitate a 'data-centric' DoD in which data must be 'VAULTIS': visible, accessible, understandable, linked, trustworthy, interoperable, and secure. It highlights the goal of making data interoperable across military domains (page 10) which would have significant implications for all-domain operations and military operations.

In The US National Strategy for Critical and Emerging Technologies, the US outlines two pillars: (1) 'To Promote the National Security Innovation Base' — focusing on skills development and the creation of a strong US private-public partnership; and (2) 'Protect Technology Advantage' — protecting US intellectual property and research and development innovation from adversarial actors. The document provides a high-level expression of strategic intent and highlights 20 priority technology areas including artificial intelligence, quantum information science, and space technologies.[14]

Finland published its positions on public international law in cyberspace

'The special features of cyberspace may raise questions relating to the practical application of certain provisions of public international law. It is therefore important to take part in close international cooperation and to exchange views about how, in certain questions, international law regulates States'

[14] The Whitehouse: Statement from the press secretary regarding the national strategy for critical and emerging technologies

use of information and communication technologies. That is why Finland is now joining the group of States that have publicly expressed their positions on international law in cyberspace.' (Ministry for Foreign Affairs of Finland, 15 October 2020)

Finland has released its official position[15] on the applicability of international law in cyberspace, joining the list of countries who have already expressed their views on the matter (see the list in the CCDCOE Strategy & Governance repository [16]). More countries have indicated that they are preparing to follow suit. In addition to reinforcing the applicability of international law in the cyber environment, such action also contributes to the formation of customary law by shaping the *opinio juris* – understanding of the behaviour expected of States.

Finland's statement underscores that cyberspace is not a 'Wild West' and points out that such claims are contrary to the established consensus at the UN. [17] The position recognises the applicability of, *inter alia*, the UN Charter – including the sovereign equality of states, the prohibition of the use of force, the peaceful settlement of disputes, the prohibition of interference in internal affairs and respect for human rights – to activities in cyberspace. Notably, Finland principally views non-consensual intrusions into digital infrastructure in another State's territory as violations of international law, which trigger State responsibility. It also recognises that States have a due diligence obligation to not knowingly allow their territory to be used to cause significant harm to the rights of other States.

Finland recognises that a cyberattack with the scale and effects corresponding to those of an armed attack justifies a response in self-defence, pointing out some debated questions such as severe economic effects and indirect or long-term effects of the cyberattack. It also stresses that any interpretation of the use of force in cyberspace should respect the objectives and purpose of the UN Charter to prevent the escalation of armed activities: responses to such severe cyberattacks, whether by cyber or armed action, must not be disproportionate or excessive. For cyber operations that are part of, or amount to an armed conflict, the rules of international humanitarian law apply. This means that cyber means and methods of warfare must be used consistently with the principles of distinction, proportionality and precautions, and care shall be taken to ensure the protection of civilians and civilian objects, including essential civilian infrastructure, services and data.

Cyberspace Solarium Commission takes stance on China in Supply Chain Security whitepaper

'Over the past two decades, China has mobilized state-owned and state-influenced companies to grab a dominant position in markets for several emerging technologies, including the market for telecommunications equipment.' (Cyberspace Solarium Commission, 19 October 2020)

The Cyberspace Solarium Commission is a US strategic cyber defence entity tasked with the development of strategic approaches to defend the US in cyberspace. The commission has released several reports and white papers on such topics as the federal cyber workforce and cybersecurity lessons from the pandemic. The latest publication, published on 10 October, is a whitepaper titled 'Building a Trusted ICT Supply Chain'.[18]

It identifies a problem arising due to China's efforts and government-led industrial policies, trade practices and intellectual property theft and points out the lack of a coherent and cohesive overarching US strategy to secure ICT supply chains. The paper proposes key points to archive a trusted supply chain, namely (1) the identification of key technologies and risks; (2) strategic investment for minimum manufacturing capacity; (3) protection of supply chains through intelligence sharing and testing; (4) investment in infrastructure to stimulate the domestic market and; (5) global competitiveness towards China's anti-competitive behaviour.

[15] Ministry of Foreign Affairs of Finland: International law and cyberspace: Finland's national positions
[16] CCDCOE Library: Statements on international law
[17] Ulkoministeriön Blogit: Kybertoimintaympäristö ei ole villi länsi
[18] Cyberspace Solarium Commission

The proposals by the Commission seem to be in line with US stance and actions towards previously reported on topics like TikTok, WeChat, Huawei and ZTE with the significant difference of not concentrating on individual Chinese companies, but rather focusing on Chinese trade policies as a whole. If the US government adopts the points set out in the whitepaper, current tensions may see another spike.

4. Recent guidelines and recommendations

US NSA issues warning against Chinese State-Sponsored Actors Exploiting Publicly Known Vulnerabilities

'The US National Security Agency is warning that Chinese-linked hacking groups are exploiting 25 vulnerabilities in software systems and network devices as part of cyberespionage campaigns - which means patching is urgent.´ (InfoRisk Today, 21 October 2020))

On 20 October, the US National Security Agency (NSA) published a cybersecurity advisory detailing the top 25 vulnerabilities being exploited by Chinese state-sponsored actors. In this advisory, the NSA noted that Chinese state-sponsored malicious cyber activity is one of the greatest threats to US National Security Systems (NSS), the US Defense Industrial Base (DIB), and the Department of Defense (DoD) networks.

Most of the vulnerabilities listed in the advisory can be exploited to gain initial access to victim networks using products that are directly accessible from the internet and act as gateways to internal networks. The majority of the products are either for remote access or for external web services. The list includes vulnerabilities in Microsoft Windows and other products and services such as Pulse Secure VPN, F5 BIG-IP proxy/load balancer, Citrix ADC/Gateway, MobileIron MDM, Adobe ColdFusion, Oracle WebLogic/Fusion and Cisco IOS XR. The NSA recommends organisations prioritise patching these vulnerabilities. Military organisations often use and depend on commercial off-the-shelf products like these and therefore need to consider these recommendations just as seriously as organisations in other sectors. Effective certification processes before fielding equipment are important and should consider the supplier's processes for managing vulnerabilities and issuing security updates.

Besides the vulnerabilities and corresponding mitigation actions announced by national cybersecurity agencies and Cyber Security Incident Response Teams (CSIRTs), the majority of hardware and software vendors have been posting their security reports on their websites to give customers up-to-date security updates.

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