CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Recent Cyber Events and Possible Implications for Armed Forces

#3 – June 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

APT uses one breached government organisation to attack others

'After five years under the radar, the Naikon APT group has been unmasked in a long-term espionage campaign against several governments in the Asia-Pacific region. […] Specifically targeted are government ministries of foreign affairs, science and technology, and government-owned companies.' (Threatpost, 7 May 2020)

'Interestingly, the group has been observed expanding its footholds on the various governments within APAC by launching attacks from one government entity that has already been breached, to try and infect another.' (Check Point Research, 7 May 2020).

The modus operandi of this APT is interesting and clearly shows how defence in depth is important and how even otherwise trusted parties can pose a risk of malware infections. For example, the Check Point report mentions an embassy unknowingly sending malware-infected documents back to its home country.

Since the cybersecurity posture of different organisations can vary a great deal, this tactic may be effective in reaching targets that may otherwise be difficult to breach.

Air-gapped systems not as secure as one may believe

'Cybersecurity researcher Mordechai Guri from Israel's Ben Gurion University of the Negev recently demonstrated a new kind of malware that could be used to covertly steal highly sensitive data from air-gapped and audio-gapped systems using a novel acoustic quirk in power supply units that come with modern computing devices.' (The Hacker News, 4 May 2020)

Air-gapped[1] systems are common in military installations and national security systems and are generally considered much more secure than systems connected to the internet or other public networks.

The article quoted above is one example of how information may be exfiltrated from an air-gapped system. Over the years, researchers have presented several similar techniques using radio waves, light or sound generated by malware. Even though not all these techniques are practical in every situation,[2]

[1] Air-gapped refers to a computer or network of computers with no network connection to any other systems. The lack of network connections makes such systems more difficult to reach for an attacker.

[2] The methods generally have low bandwidth and require relative physical proximity of the equipment receiving the data.

they show that information in an air-gapped system is not necessarily secure if malware can be placed on the system.

Stuxnet was an early example of the risk of attacks against air-gapped systems. Every system needs external inputs, even if it is not connected to other networks, and is therefore susceptible to malware attacks. The malware can be introduced on removable media like USB-drives containing data or software or on computers temporarily connected to the air-gapped system.

Current examples of malware targeting air-gapped systems include Ramsay [3] and USBferry. [4] The fact that they have mechanisms to replicate through removable drives indicates that they are intended to work on air-gapped networks. USBferry, in particular, is believed to be used against military targets. Another example is the malware USBCulprit which is said to rely on USB media to exfiltrate data from air-gapped systems.[5]

This highlights the need for the adequate protection of air-gapped systems. Preventive measures against exfiltration can include TEMPEST protection, protection against audio and visual eavesdropping, and strict control of computer media leaving the system. Effective controls are also needed to prevent the infiltration of malware. Recommended options include standard antivirus controls on media for software updates and data import, and measures addressing supply-chain risks such as verifying the authenticity of software and updates. User training is essential, as not all users may be aware of the ways air-gapped systems can be compromised. Last, but not least, one should not forget the insider threat.

What do Russia's plans for navigation services tell us about the risk of GPS jamming?

'Russia regularly jams GPS signals in northern Scandinavia. The government often "spoofs" receivers in Moscow and elsewhere into thinking they are tens of kilometers from their true location. It is no surprise then that Russia's five-year radio navigation plan focuses so much on countering such threats for its citizens and military forces.' (C4ISRNET, 20 April 2020)

The fact that Russia is expecting jamming of satellite positioning systems does not come as a surprise. Russia has been accused of interfering with GPS, for example jamming the system during NATO exercises as seen in Norway during Trident Juncture in 2018. [6] Naturally, loss of GPS signals increases the likelihood of navigational errors for civilian and military air and sea traffic alike, with unmanned systems affected most severely. Russia's plans to counteract this type of attack reinforce the picture of this being an offensive capability that would be used in a conflict.

Measures mitigating this can include, as in Russia's plans, terrestrial-based navigation systems as a complement and backup, and developing more robust satellite-based systems.

Hacked defence contractors could mean risk to the military

'Britain's Ministry of Defence contractor Interserve has been hacked, reportedly leaking the details of up to 100,000 of past and current employees, including payment information and details of their next of kin.' (The Register, 15 May 2020)

'The huge cyberattack last year against Mitsubishi Electric Corp likely leaked information related to one of the most advanced weapons being developed, government sources said.' (*The Asahi Shimbun*, 20 May 2020)

Employee information leaked from defence contractors could potentially aid an adversary in targeting individuals with access to sensitive information, installations or operations. The risk related to leaked weapon systems data is obvious, and even non-classified information could potentially aid adversaries in, for example, assessing capabilities and designing countermeasures.

Targeting a contractor rather than the military or a ministry or government authority is, of

[3] ThreatPost: Ramsay malware targets air-gapped networks; ZDNet: New Ramsay malware can steal sensitive documents from air-gapped networks
[4] ZDNet: Hackers target the air-gapped networks of the Taiwanese and Philippine military
[5] The Hacker News: New USBCulprit espionage tool steals data from air-gapped computers
[6] The Barents Observer: Pilots warned of jamming in Finnmark; GPS World: Norway, Finland suspect Russia of jamming GPS

course, a tactic often used to circumvent the sometimes better cyber defences of those organisations. It is important to ensure that contractors have an adequate cybersecurity posture. Procedures for notification of security breaches of contractors are also important so that mitigating action can be taken as quickly as possible.

Increasing use of autonomous operations may make the military more vulnerable to cyber attacks

'The effect that the COVID-19 pandemic is having on military readiness and the possibility—even probability—of future pandemics will increase the emphasis on networked autonomous operations in the Army.' (Strategic Studies Institute, 30 April 2020)

Military operations in the future will likely rely more on unmanned and autonomous systems which in turn will rely heavily on computer and communication systems and therefore be susceptible to cyber-attack and electronic warfare effects. The lack of human presence will make backup solutions that do not depend on data communication much more difficult to implement. Consequently, the cybersecurity of the systems is more important than ever before.

The Cyberspace Solarium Commission[7] has made recommendations on securing weapon systems. In an article from the Centre for Strategic International Studies (CSIS), it expands on them and stresses the need for cybersecurity to be an integral part of the acquisition process.[8]

2. Other cyber activities relevant to the military

Research facilities targeted by state actors may affect defence research

'Hostile states are attempting to hack British universities and scientific facilities to steal research related to Covid-19, including vaccine development, cybersecurity experts have warned. The National Cyber Security Centre (NCSC) said the proportion of such targeted cyber-attacks had increased, branding the criminal activity "reprehensible". It is understood that nations including Iran and Russia are behind the hacking attempts, while experts have said China is also a likely perpetrator.' (*The Guardian*, 3 May 2020)

In addition to the reports of attempts to steal research, there are reports from Israel of targeted cyber-attacks to sabotage vaccine development.[9] There have also been reports of attacks against several supercomputer centres, first reported in Germany and the UK. [10] In addition to the risk to medical research which could affect the whole of society, attacks could have effects on other research. These resources are often used for a wide range of purposes, defence research included.

Later reports say there are indications that the object of the attacks on supercomputer facilities was to mine cryptocurrency rather than to affect specific research.[11] Either way, the attacks would reduce the availability of the supercomputing resources, and therefore potentially affect research of value for the military and national security.

What does your car know about you and where does that information end up?

'Tesla infotainment systems are a marvel to behold. Among other things, they display Netflix or YouTube videos, run Spotify, connect to Wi-Fi, and of course store phone numbers of contacts. But those benefits require storing heaps of personal information […] The researcher […] recently gained access to 13 Tesla [media control units] that were removed from electric vehicles during repairs and refurbishments. Each one of the devices stored a trove of sensitive information despite being retired.' (ArsTechnica, 6 May 2020)

---

[7] Cyberspace Solarium Commission
[8] CSIS: Prioritizing weapon system cybersecurity in a post-pandemic defense department
[9] The Times of Israel: Israeli vaccine research centers reportedly among sites targeted by hackers
[10] DefenseWorld.net: Supercomputers in research institutes across Germany, UK hacked
[11] ZDNet: Supercomputers hacked across Europe to mine cryptocurrency

Modern cars have advanced navigation and infotainment systems that can accumulate large amounts of potentially sensitive information about where the vehicle travels, who the driver is communicating with and so on. This information may be transmitted to the car manufacturer or third-parties as the car 'calls home', but as the article cited above shows, the information may also end up in parts swapped out during repairs and maintenance of the vehicle.

As military organisations use COTS vehicles, military vehicles based on civilian products and vehicles maintained by civilian contractors, these vulnerabilities will affect the military too. The onboard systems of a car may contain information about the locations of classified installations, or the movement of sensitive personnel or in covert operations.

These risks must be continuously assessed and preventive measures taken. The right mode of transport should be chosen for sensitive operations and procedures put in place to ensure that any information-bearing components taken out of a vehicle are disposed of securely.

Old vulnerabilities still exploited; patching will protect you

'As of December 2019, Chinese state cyber actors were frequently exploiting the same vulnerability—CVE-2012-0158—that the U.S. Government publicly assessed in 2015 was the most used in their cyber operations. This trend suggests that organizations have not yet widely implemented patches for this vulnerability and that Chinese state cyber actors may continue to incorporate dated flaws into their operational tradecraft as long as they remain effective.' (US-CERT 12 May 2020)

The most used vulnerabilities can all be mitigated by either applying security patches, upgrading to a later version or following the best practice and vendor recommendations regarding the security configuration of products.

This clearly shows that keeping software up to date and applying recommended security configurations are still the most effective way to raise the bar for an attacker to breach the security of information systems. For the most sensitive systems, and to protect from the most resourceful adversaries, this will not be enough; but as long as connected systems are not patched, the more advanced protections may not be of any use.

Whether patches can be applied quickly or not depends on the characteristics of the system in question. For some systems where a loss of functionality for a limited time is acceptable, it may be most effective to apply patches from trusted software vendors immediately without thoroughly testing and addressing any reliability issues when the patches have already been rolled out. In cases where the reliability and availability of the system are paramount and failure may lead to failed operations or even loss of life, patches must be well-proven before deployment. In cases where there is a considerable risk that the vulnerability may be exploited and the necessary testing will take too long, other means of mitigating the risk should be considered. Good cyber assurance programs continually need to be reviewed, balancing risk and the functionality of the systems they are designed to protect.

Iranian port targeted in cyber-attack

'Israel was behind a cyberattack that disrupted a major port in Iran, done in response to an attempt by the Revolutionary Guards to infiltrate an Israeli water facility.' (*The New York Times*, 19 May 2020)

Ports, railroads, airports, locks and bridges are crucial for military mobility. They are all, in one way or another, dependent on cyber infrastructure and vulnerable to cyber-attacks. Attacks on civilian infrastructure, such as ports in this case or water supply as in the failed attack on Israel in April, will potentially affect military operations. It is a national security interest to protect critical infrastructure, as this is a necessary foundation for both civilian and military capabilities and will be targeted using cyber means in a hybrid conflict.

The attack could be a part of a continuing cyber conflict between Israel and Iran, with the attack against the Iranian port being a message from Israel regarding the attempted

attacks against the Israeli water distribution system.[12]

Attacks against ports may carry particularly high risks, since only a few major ports in, for example, Europe are responsible for a large proportion of the total port capacity. Many states do not own the port capacity they need for their supply lines, but are dependent on ports in other countries and, in many cases, privately owned operators in those ports.

Although there may be no active disruptive attacks against NATO's or allies' critical infrastructure at the moment, compromises that are part of preparations for such attacks may be ongoing. German intelligence and security agencies have reportedly warned about the activities of the hacking group Berserk Bear, previously linked to Russia, against companies in the energy, water and power sectors.[13] Such attacks could include reconnaissance and getting and maintaining a foothold for future operations in the targeted infrastructure.

3. Policy and strategy developments

Executive Order on Securing the United States Bulk-Power System

'This week President Trump signed an executive order that prohibits operators of US power grids to buy and install electrical equipment that has been manufactured outside the US. […] President Trump is aware of the efforts of foreign adversaries that are increasingly targeting US power grid by creating and exploiting vulnerabilities in the US bulk-power system. The power grid provides electricity that supports national critical infrastructure, for this reason, foreign threat actors are increasingly targeting them.' (Security Affairs, 2 May 2020)

The executive order[14] is not a complete ban but directs the Secretary of Energy and others to determine if there are undue or unacceptable risks.

President Trump has also extended his executive order banning US companies from using or buying telecoms equipment from Chinese manufacturers Huawei and ZTE for another year.[15]

A similar development in Estonia is the amendment of the Electronic Communications Act.[16] This will authorise the government to introduce an obligation to provide information about the technology used in communications networks to ensure a high level of security. In this case, foreign equipment is not singled out, but it will allow government oversight over what equipment is used.

Domestic products or products produced by allies are generally considered more secure. Assessing the risks is, however, not easy, considering that high-tech products in almost every case contain components of different origins on which many different actors in different countries have an influence. 'Made in the USA' may only mean assembled in the USA. The risk management approach indicated in the policies is important, but applying it to 'domestic' products is also recommended. Selecting the products that pose the least risk can be combined with building security architectures that are as robust as possible against individual components that may be compromised.

NATO expands its cyber defence capabilities

'NATO is doubling down on cyberspace defense with increased partnerships and new technology thrusts. Information exchanges on threats and solutions, coupled with research into exotic capabilities such as artificial intelligence, are part of alliance efforts to secure its own networks and aid allies in the cybersecurity fight.' (AFCEA SIGNAL, 1 May 2020)

NATO has its own cyber defence capabilities protecting the organisation's networks and information systems and uses its own staff rather than relying on personnel from the member nations.

---

[12] *The New York Times*: Israel hack of Iran port Is latest salvo in exchange of cyberattacks; Al-Monitor: Israel response to cyber attack sends clear warning to Iran

[13] CyberScoop: German intelligence agencies warn of Russian hacking threats to critical infrastructure

[14] The White House: Executive order on securing the United States bulk-power system

[15] The Register: Donald Trump extends ban on Huawei, ZTE telecoms kit in US companies to May 2021

[16] Riigikogu: Amended electronic communications act

SIGNAL talked to Christian Lifländer, head of the Cyber Defence Section of NATO's Emerging Security Challenges Division. Lifländer stresses the partnered approach to NATO's cyber defence and the need for cooperation with the allies and with industry. Information sharing is essential, as malicious cyber activity in NATO networks can almost certainly be found in nations' networks as well.

AI is already a component in the defence of NATO networks, and as NATO is expanding its cybersecurity capabilities the organisation will be looking at both the use of and defence against AI and other emerging technologies.

Tech and telecom companies call for open 5G systems

'More than 30 technology and telecom firms unveiled an alliance Tuesday to press for "open and interoperable" 5G wireless systems that eliminate the need for a single supplier. The move comes amid heightened global debate over politically sensitive deployment of the ultrafast fifth-generation networks in a market led by Chinese-based Huawei, along with European-based Nokia and Ericsson. The new Open RAN Policy Coalition said an open-standards system with competitive bidding for various components in a "radio access network" would avoid depending on any single technology supplier.' (Breitbart, 5 May 2020)

A new coalition of users of 5G technology has formed, advocating standardisation. [17] 5G networks will, of course, increasingly be part of military systems and civilian infrastructure used by the military. Concerns about the influence of Chinese suppliers on these systems have been discussed. The new coalition addresses the issues related to the part of the 5G infrastructure called a Radio Access Network (RAN). [18] Unlike other protocols in the 5G technology, the protocols and interfaces between sub-components of the RAN are not standardized. This means software and components from different vendors cannot be mixed and matched.

Using standards to ensure that there is no lock-in to one supplier would also be a benefit for building secure systems. With the ability to pick trusted suppliers for critical parts of the architecture, it may be possible to isolate the effects of other less trusted components in the system. Standards will also make it easier to swap one product for another if a vulnerability is found without having to redesign an entire network or change the supplier of every part of the system. Influencing standards, and collaborating with international partners on research and standards is also stressed in the US Department of Defense 5G Strategy.[19]

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

[17] Open RAN Policy Coalition: Open RAN Policy Coalition launches to advance open and interoperable solutions to expand the global advanced wireless supply chain

[18] The Radio Access Network (RAN) consists of the cell sites and their subcomponents such as radios, hardware and software that end user devices communicate with.

[19] Department of Defense (DoD) 5G strategy