CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

No 11 / June 2021

Recent Cyber Events:

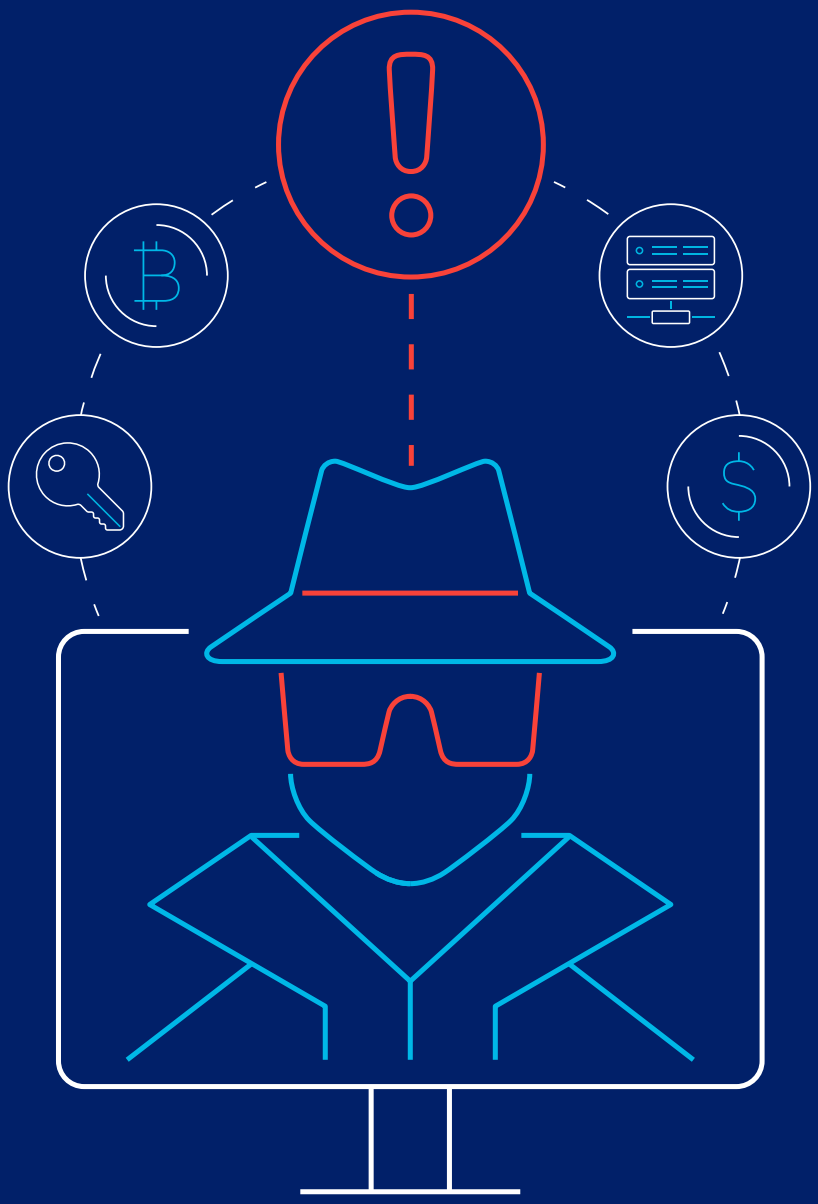
Considerations for Military and National Security Decision Makers

Ransomware:

- → The Colonial Pipeline Attack
- → Ransomware Attack Against Irish Health Care
- → Ransomware and Cyber Insurance

Other topics in this issue:

- → Executive Order on Improving US Cybersecurity
- → UN's Open-Ended Working Group and Programme of Action
- → Blockchain for Military Applications



Published by CCDCOE

ABOUT THIS PAPER

This recurring report is the collaborative view of NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) researchers highlighting the potential effects of current events and developments in cyberspace on armed forces, national security and critical infrastructure, 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.

Colonial Pipeline: Ransomware attack causes fuel shortage

On 7 May, the Colonial Pipeline, a US company operating a system of pipelines responsible for distributing nearly half of the fuel to the American east coast, was hit by a significant ransomware attack. In its response to the attack, the company shut down the operation of the pipeline for several days leading to fuel shortages in affected states resulting in widespread hoarding of gasoline and an increase in fuel prices.

'Before an attack, we carefully analyze your accountancy and determine how much you can pay based on your net income. You can ask all your questions in the chat before paying and our support will answer them.' (The DarkSide ransomware gang as reported by Kim Zetter)

Although this attack has been attributed to a criminal organisation and not a state actor, it clearly shows the significant effects even a single attack can have on society. State actors are generally considered to have superior capabilities to criminal organisations. Attacks such as these from state actors are certainly possible and could easily masquerade as criminal activity to maintain deniability from the responsible state.

Questions may be asked regarding the level of preparedness of an organisation like Colonial Pipeline to protect against and respond to an attack like this. In this case, a leaked password to a VPN account seems to have been the way into the network, but unpatched vulnerabilities are often exploited in this type of attack. Keeping systems up-to-date and correctly configured may not stop a determined well-funded attacker or one with access to a password, but it will raise the bar significantly. Two-factor authentication may be the most effective measure against compromised passwords.

In the case of Colonial Pipeline, it has been reported that only the business network, not the operational network responsible for running the pipeline, was affected by the ransomware. This indicates a segregation between the two networks, which is good security practice. The operational network and the pipeline were nevertheless less shut down as a precaution, possibly to protect them from also being affected by the ransomware. Taking measures to contain the attack and prevent further spread is considered good practice, but in this case, it resulted in an essential service in effect being shut down. For a critical service such as fuel distribution, business continuity and disaster recovery plans should be in place and should ensure that an attack can be handled with minimal impact on the service. We cannot say exactly what could have been done in this particular case, but planning must consider a complete shutdown or failure of the 'office network' so that procedures are in place to secure other systems and to continue production while the business network is restored from back-ups kept safe from the ransomware.

It is also important to stress the significance of reviewing and exercising these plans regularly; exercises should not be limited to the technical personnel. Decision makers at all levels need to practice to ensure that they are prepared to make the right decisions during a crisis. Procedures should be tested and any limitations at the technical level in implementing the business continuity and disaster recovery plans need to be found so that they can be addressed.

The attack also raises the question of how to bring the culprits to justice. An attack like this is illegal in most jurisdictions, but since it is cross-border it is in practice very difficult to police. The group thought to be responsible for this attack, like so many of these gangs, is believed to be based in Eastern Europe, possibly Russia. As long as Russian interests are not harmed, the state is thus far said to turn a blind eye to their activities. According to the Tallinn Manual 2.0, there is a broad consensus that failure to curtail criminal activity from your territory may not be

considered responsible behaviour. When the attack causes actual harm to critical infrastructure, the question arises whether there would be an obligation under international law for Russia to take action and what can be done to bring about a change.

Finally, there is the question of whether to pay the ransom or not. Although the FBI, CISA and many others clearly recommend not paying a ransom, Colonial Pipeline is reported to have authorised a $4.4 million payment only to find out that restoring this way was too slow. The US Department of Justice has been able to follow the money by reviewing the Bitcoin public ledger, showing the value of reporting attacks to the proper authorities. Remarkably, they were also able to recover about half of the ransom payment. More on ransom payments to ransomware attackers in the article on cyber insurance in this paper.

Ransomware attack against Ireland's Health Service Executive (HSE)

On the night of Friday, 14 May 2021, the HSE, Ireland became aware that they were victims of a 'significant and sophisticated' ransomware attack.

Ransomware attacks against the health care sector are particularly troublesome since they may disrupt medical services. In this case, some hospitals had to cancel routine appointments. While no personal information seems to have been compromised, the attack shows that the risk cannot be ignored. The risks to the integrity of medical data must also be considered; an attack that could change medical records could have severe consequences.

'[that the cost of this] will be in the tens of millions and there is no doubt that €100 million will be the small figure in terms of the total cost of this' (Paul Reid, CEO of HSE, 21 May 2021)

Ireland's National Cyber Security Centre has been assisting the HSE in managing the response to this attack. Along with cybersecurity consultants, FireEye, they have been working 24-hour shifts on a decryption key supplied by the criminal gang. The Conti Ransomware which infected the HSE network is the product of a group of cybercriminals known as Wizard Spider. The Irish Government, for its part, refused to pay the ransom and instead issued a court injunction against the Conti hackers to prevent HSE data exposure or sale on the Dark Web. This stance is to be commended.

'It is also the case that paying a ransom may simply push the price up, not just for this attack but for the next one and one after that. It would send a message that Ireland is prepared to pay, so why wouldn't other, similar criminal groups try their hand at extorting us?' (Eamon Ryan, Minister for the Environment, Climate and Communications, 18 May 2021)

There has, however, been some commentary that there has been an under-investment in cybersecurity and defence over recent years. Of course, it is commonly accepted that no system can be 100% secure or protected, but the latest thinking is that there must be a significant cost imposed to deter adversarial actors. Ireland must be prepared to address this if it wishes to secure its title as 'data capital of Europe'.

Ireland may receive sympathy for this crippling attack on its health care system, and though there are a plethora of ransomware cyberattacks across the globe at the moment, it will be wise to ensure that cybersecurity policies and defence-in-depth measures are dramatically improved across the wider public service.

Cyber Insurance provider hit by ransomware attack

Ransomware has been a dominant topic in the cybersecurity community during the pandemic and a great number of ransomware attacks have been covered in the news. According to Blackfog, research suggests that in 2020 cyber criminals carried out ransomware attacks against businesses every 11 seconds and that monetary damages will be at about $20 billion in 2021. Last year, the country with the highest number of reported attacks was the United States, followed by the United Kingdom, Australia, Canada, and Germany.

While many news articles focus on ransomware attacks against industry and private companies, the military and critical infrastructure have also suffered attacks. Cybertalk recently published an article covering an attack against a US Air Force contractor producing platforms for weapon systems and machinery transport.

'"We are on the cusp of a global pandemic," said Christopher Krebs, the first director of the Cybersecurity and Infrastructure Security Agency, told Congress last week. The virus causing the pandemic isn't biological, however. It's software.' (AXIOS, 11 May 2021)

Ransomware attacks typically encrypt computers and servers and sometimes spreads to all devices in a network rendering them useless until a key is entered to unencrypt them. This often means that everyday operations cannot be carried out until the cyber hostage-takers receive payment. In certain cases, ransomware attackers can also underline the seriousness of their intent by leaking parts of sensitive data online, visible to the whole internet. For many businesses, the loss of operational capabilities alone equals a loss in revenue and thus the pressure to regain

control over its devices is high.

There are ways to regain control without paying the ransom by using back-ups and by rolling devices back to a point before the ransomware attack was carried out. This, however, would require that proper safeguards were in place so that the back-ups themselves were not affected by the attack and were not encrypted.

As the attack against the US Air Force contractor shows, ransomware attacks can become a supply chain issue and thus have repercussions for military operations, even if the military itself was not directly targeted. A delay caused by a contractor not delivering in time could cause a ripple effect throughout the whole supply chain and leaked data could potentially give an adversary unwanted information about capabilities and plans.

Notwithstanding the question of whether or not to pay a ransom, one way of being able to resume operations quickly is to rely on cyber insurance, which, depending on the specifics of the contract, would cover ransom costs. This means that the attackers could be paid quickly and the company reimbursed. In recent developments, CPO Magazine reports that one of the biggest insurance providers in the world, AXA, announced that they would stop covering reimbursements of ransomware payments for customers in France. While some customers will still be covered by the insurance due to the terms of their contracts, AXA will no longer be offering this type of insurance. The reason for this change is reportedly a French Senate meeting in which officials discussed the possibility of making ransomware payments illegal, something that is also being debated in the US. Chris Painter, co-chair of the White House-backed Ransomware Task Force (RTF), says that a ban on paying ransoms would have to be implemented incrementally and be combined with measures to help protect potential ransomware victims.

The Daily Swig reports that shortly after the AXA announcement, the insurer was hit by a ransomware attack against its Asia Assistance division. Reportedly three terabytes of data including personal data were stolen.

To prevent ransomware attacks, not only is adequate cybersecurity awareness in personnel needed so that phishing emails are less effective, but proper asset management of outdated and vulnerable IT equipment is vital. Technological and software measures such as endpoint security and secure email gateways can be implemented so that the threshold for a successful attack is even further raised. There is also a clear need for improved cybersecurity in supply chains. When going into business with a contractor or third party, it is important to establish strict security requirements covering cyber awareness training for employees and measures against cyberattacks such as ransomware.

The Biden Administration's Executive Order on Improving US Cybersecurity

'The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy.' (Executive Order on Improving the Nation's Cybersecurity)

The Biden Administration released a new order on 12 May 2021 containing measures to improve national cybersecurity. The cyberattacks affecting society and national security such as the Colonial Pipeline attack, the SolarWinds attack on the software supply chain, the hacking of the emails of US businesses and military contractors have caused the US government to take this step.

Many important issues such as increasing threat information sharing between the private sector and government agencies, modernising the cybersecurity infrastructure of public institutions, improving software supply chain security and establishing a new cyber safety review board with private sector representatives under the head of Homeland Security, are addressed in the executive order.

One of the most striking aspects of the order is that it supports the transition from the classic data center approach to using secure cloud-computing environments and adopting a zero-trust architecture[1]. It is thought that the transition to cloud architecture, using technologies such as SaaS and PaaS, is inevitable in the future, and may help in implementing security architectures such as zero-trust more quickly and efficiently. Therefore, the focus of the report on this area is considered positive.

It may not be possible to solve the problems that have been going on for years, especially in sharing information between the public and the private sector, in a short time with this order. Private sector companies in the US do not, in general, have any legal obligation to report cyber incidents other than those involving personally identifiable information. For this reason, changes may need to be made in the laws for the order to be implemented efficiently.

The rapid reaction of the agencies that will take part in the execution of the order, the willingness of the private sector and the effective functioning of the new security board will contribute to an increase in the US national cybersecurity level. However, these measures alone will not be sufficient and new measures will be needed in the constantly changing threat environment. In addition to

1 Zero-trust refers to a paradigm where it is assumed that attackers are present both inside and outside traditional network boundaries and implicit trust in devices on users based on physical or network location (e.g. on a local network as opposed to on the internet) is eliminated. For more information see NIST SP 800-207.

the internal measures of the countries, close cooperation and information sharing between allied countries will also make a significant contribution to the increase of the cybersecurity levels of all allies.

United Nations Open-Ended Working Group and Programme of Action

State use of information and tele-communication technologies (ICTs) was brought to the attention of the United Nations (UN) in 1998 when the first resolution was tabled by the Russian Federation. It called on states to address the issues which ICT threats could pose and suggested developing principles to enhance security.

Discussions on the state use of ICT quickly took the form of a Group of Governmental Experts (GGE) under the Disarmament and International Security Committee. Thus far, there have been five GGEs that have agreed on three consensus reports (2010, 2013 and 2015) which form a framework on responsible state behaviour in cyberspace. It has four elements: voluntary and non-binding norms of responsible state behaviour; international law; confidence-building measures; and capacity building.

This framework aims to guide states on which kind of behaviour is acceptable in their use of ICT to increase trust, predictability and transparency.

In 2017 the fifth GGE did not reach consensus and a resolution was tabled which created a sixth GGE consisting of 25 experts. An additional group was also created – the Open-Ended Working Group (OEWG) which discussed the same elements of the framework for responsible state behaviour but allowed all UN member states to participate. In the first half of 2021, the sixth GGE and the OEWG wrapped up their respective work programmes. In March the first-ever OEWG adopted its consensus report, which reaffirmed the importance and value of the GGE reports from 2010, 2013 and 2015.

During the OEWG negotiations, one of the key topics was on regular institutional dialogue, meaning how and in what format states would discuss the framework of responsible state behaviour under the auspices of the UN.

By the final meeting of the OEWG, an additional resolution had been tabled by the Russian Federation to create a second OEWG with a five-year mandate until 2025. However, as many member states do not see the OEWG format as the preferred option, a joint contribution was presented called 'The future of discussions on ICTs and cyberspace at the UN' in which forty-seven states call for the creation of a Programme of Action (POA) to provide a permanent, inclusive and transparent framework which would work on consensus and include wider participation, including multi-stakeholder engagement while avoiding duplication of processes. It would focus on the implementation of the eleven norms of the 2015 GGE report while remaining open to topics related to the state use of ICT.

In the consensus report of the OEWG, the group brought forward a proposal to create a POA, but with the reservation that when proposals on regular institutional dialogue are presented, the concerns and interests of all states should be considered. With that, the possibility of a POA was tied with the new five-year OEWG which would elaborate on the proposal.

In the last week of May 2021, the sixth GGE adopted the fourth consensus report that 'builds upon the previous GGEs, harmonises with the OEWG report, and importantly adds a valuable new level of understanding on complex issues related to ICTs in the context of international security' as stated by the High Representative for Disarmament Affairs Ms Izumi Nakamitsu. Therefore, the current framework of responsible state behaviour will have an additional layer with the new report.

To sum up, the discussion on the lines of work under the auspice of the UN are ongoing as the organisational meeting of the new five-year OEWG took place on the first two days of June. What remains now are the efforts of states to agree on the format of discussions in the future and the areas of convergence on regular institutional dialogue.

Blockchain technology for military applications

In recent years, the term blockchain has become a more and more familiar word and with the ever-growing popularity of cryptocurrencies as investment, speculation and payment, the term has found its way into the vocabulary of communities outside the technology enthusiasts. The rise in interest and media coverage about non-fungible tokens (NFTs)[2] has again put blockchains in the limelight this year. There are however security and IT experts voicing scepticism about the usefulness of blockchains other than as a part of cryptocurrency and whether there are useful applications in national or allied defence.

Blockchain is a technology defined as a public, shared and decentralised database. These three qualities have made it become a very good solution for records, since it is unalterable. Each block in the chain depends on the previous one, so modification in one of the records would cause a cascade of modifications. For that to be carried out, all the existing copies of the database would have to

2 See Forbes for more information.

be modified. Its robustness will increase with the number of nodes[3] belonging to the network due to decentralisation.

Although its rise to fame has indeed been brought about by its application in the field of cryptocurrencies, this is only one of its many applications including cloud storage by P2P[4], management of digital identities to prevent impersonation, registration and verification of data in sales transactions or medical history, smart contracts, supply chains and voting systems.

In the military field, some of these applications are being considered for implementation. One is the application of blockchain technology in supply chains for the control of components and parts in military systems providing traceability capable of detecting unscheduled changes and giving the responsible institutions the ability to expand the range of suppliers. Another possible application is the decentralisation of message handling for protection against repudiation or denial and, in situations of attack against infrastructure, to be resilient and able to operate even when a part of the network has been compromised.

According to Fintech News, DARPA is currently working on using blockchain technology for the protection of data related to weapon systems and in 2018 Russia's Ministry of Defence announced that it was exploring capabilities to identify and prevent hacking attacks on military infrastructure. Reportedly, China started developing a military logistics system based on blockchain technology in 2016.

'In the coming years, the defence research community is expected to search for new applications for the military based on blockchain technology with predominant candidate areas such as cyber defence, secure messaging, resilient communications, logistics support and the networking of the defence Internet of Things.' (EDA: European Defence Matters, Issue 14, 2017)

This technology must be applied using robust consensus protocols. Among the most common are Ethereum, Corda, Quorum and Hyperledger. Hyperledger was developed by the Linux Foundation and, unlike the Ethereum network, operates in a way that supports private transactions and confidential contracts. In military applications, this would preserve the confidentiality of sensitive data. This allows the flow of information within a network without the need to share it with all the actors involved in a transaction, only the necessary ones. The architecture of this protocol is modular, allowing different uses to accommodate different needs through plug-and-play components such as consensus, privacy or membership services.

Blockchain protocols are increasing in complexity as new functionalities are implemented, which increases the margin of error and risk from vulnerabilities, so it is important to choose a reliable protocol that is in a state of active maintenance and support.

Cryptography and cybersecurity expert Bruce Schneier has been one of the critics of blockchain technology, arguing that the technology does not remove the need for trust, it just shifts some of it from a trust in people and organisations to a trust in technology. If that technology fails, there may be nothing we can do to save the system and there will also always be a need for trust in the people in managing the technology. With private blockchains, Schneier argues that not all the elements of blockchain technology are present and this is only a new name for old technology, namely distributed append-only data structures. In short, the solutions are considered by their critics to be inefficient, not scalable and unnecessary. The same security properties could be achieved without using a blockchain.

Another point of frequent concern is the high energy consumption of the proof-of-work algorithms used, for example, for Bitcoin. Solving the cryptographic problems needed to verify a new block in the Bitcoin chain, for example, require a lot of computational power; the complexity of the problems is required to ensure the integrity of the blockchain. These computational resources translate into a large consumption of electricity, which may be considered wasteful.

When evaluating any solution marketed as blockchain, it is important to remember that the definitions of the term vary widely, and the specific technology used may or may not include some of the properties usually associated with blockchain technology. This means that it is possible that the solution lacks some of the properties that you are looking for, but also that it may be useful even if a pure blockchain solution is not appropriate for the case at hand. It all comes down to a need to evaluate the specific technology with the specific use, looking at the requirements and properties of each and not so much at the moniker chosen to market the product.

3 A node is any system or device connected to a network.

4 Peer-to-Peer computing or networking. See XcelLab Magazine for more information.

CONTRIBUTORS

Alejandro Granja
Emre Halisdemir
Rónán O'Flaherty
Maria Tolppa
Jan Wünsche
Philippe Zotz

PREVIOUS ISSUES

This paper is part of a series of monthly reports. This issue and all previous issues are available in the CCDCOE online library.

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