# Cyberattacks as Digital Weapons against the IT Critical Infrastructure

# Case Study: Cyberattacks on IT Infrastructure of Albanian Government

## Cyberangriffe als digitale Waffen gegen die IT-Kritische Infrastruktur Fallstudie: Cyberangriffe auf die IT-Infrastruktur der albanischen Regierung

Elior Vila

Department of Informatics, University of Elbasan “Aleksander Xhuvani”
Elbasan, Albania, e-mail: elior.vila@uniel.edu.al

***Abstract* -** The rapid development of IT nowadays, has brought huge benefits with regard to fast information exchange. Governments around the world are using IT to offer online services to their citizens in order to accelerate communication and transactions. However, the cyber security of these services is often in question because of the numerous successful attacks that have taken place in recent time. Cyberattacks are being used as cyber-weapons to harm the country’s infrastructure and thus deny the critical services to its communities. The factors behind these destructive attacks may be complex and vary from financial and personal to political. This paper investigates a series of recent cyberattacks which targeted some of the most critical parts of the Albanian government IT infrastructure. A careful analysis will be performed in order to identify the reasons why such attacks were successful and what can be done in the future to preserve the security of crucial services provided daily to the citizens.

***Zusammenfassung* -** Die rasante Entwicklung der IT hat heutzutage enorme Vorteile im Hinblick auf den schnellen Informationsaustausch gebracht. Regierungen auf der ganzen Welt nutzen IT, um ihren Bürgern Online-Dienste anzubieten, um Kommunikation und Transaktionen zu beschleunigen. Die Cybersicherheit dieser Dienste ist jedoch aufgrund der zahlreichen erfolgreichen Angriffe, die in letzter Zeit stattgefunden haben, häufig in Frage gestellt. Cyberangriffe werden als Cyberwaffen eingesetzt, um die Infrastruktur des Landes zu schädigen und seinen Nutzern so die kritischen Dienste zu verweigern. Die Faktoren hinter diesen destruktiven Angriffen können komplex sein und von finanziellen und persönlichen bis hin zu politischen variieren. Dieses Papier untersucht eine Reihe von kürzlich erfolgten Cyberangriffen, die auf einige der kritischsten Teile der IT-Infrastruktur der albanischen Regierung abzielten. Es wird eine sorgfältige Analyse durchgeführt, um die Gründe für den Erfolg eines solchen Angriffs zu ermitteln und herauszufinden, was in Zukunft getan werden kann, um die Sicherheit wichtiger Dienste zu gewährleisten, die den Bürgern täglich zur Verfügung gestellt werden.

## I. Introduction

With the IT technological development come increased risks and security threats and never has this been truer than in today’s society. The rapid grow of online services and broad accessibility in general, created an insecure environment for the storage and processing of sensitive data. The delivery of many critical services in sectors such as food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials etc. is nowadays totally dependent on the IT infrastructure availability for information and data exchange.

Cyber-attacks are an even more significant threat to infrastructure, both public and private. Periodic reports provide timely information about security issues, attacks and vulnerabilities [1]. Cyber-attacks in various forms have become an international problem. Some cybercrime organizations and probably state actors behind have transformed these attacks into cyber weapons which are low-cost, low-risk, highly effective and easily deployable globally. With this new class of weapons, are targeted critical IT infrastructures of private and governmental institutions of countries around the world. Cyber weapons are software used to attack other software or data within computer systems [2].

The use of offensive cyber operations by nation-states directly against another state has become common motivated recently by military conflicts and sometimes political collisions. Nation-states and non-state actors may have unmatched espionage and surveillance capabilities to inflict tremendous damages on the critical assets of their targets. Progressively, non-state actors including commercial entities are developing cyber defense capabilities that were solely held by a handful of state actors in the past. Such entities have started to evaluate the risks factors as forerunners for criminal financial gain, destruction and disruption operations.

According to the latest Microsoft Digital Defense Report 2022, nation state actors are launching increasingly sophisticated cyberattacksto evade detection and further their strategic priorities [3].

## II. Threats and Attacks to Critical Infrastructures

### A. *Types of countries' critical infrastructures*

According to the According to Cybersecurity and Infrastructure Security Agency (CISA), there are basically 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the US that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof [4]. Some of these are Chemical Sector, Communications Sector, Critical Manufacturing Sector, Defense Industrial Base Sector, Emergency Services Sector, Energy Sector, Financial Services Sector, Government Facilities Sector, Healthcare and Public Health Sector, Information Technology Sector, Nuclear Reactors etc. More or less the same is true for other countries as well. An amount of sectors are heavily dependent upon IT and communication services. Therefore it is of vital importance for any country to know how to manage risks, improve security, and aid the implementation and execution of protective and response measures across the IT Sector.

### B. *Increasing attacks to critical infrastructure*

For many organizations the IT infrastructure has become increasingly reliant on connectivity. This rising trend has forced organizations to adapt and rely heavily on remote access to ensure continuity. On the other side, attackers are continuously looking for vulnerabilities to exploit and gain unauthorized remote access to valuable targets. When critical infrastructure fails, the effects can be wide-reaching and devastating for any organization or individual.

The data from Microsoft Digital Defense Report 2022 shows that cyberattacks targeting critical infrastructure during the past year increased from 20% to 40%. This trend was due to the hybrid war both in physical and cyberspace that Russia started in February 2022 against Ukrainian infrastructure, and aggressive espionage targeting of Ukraine's allies.

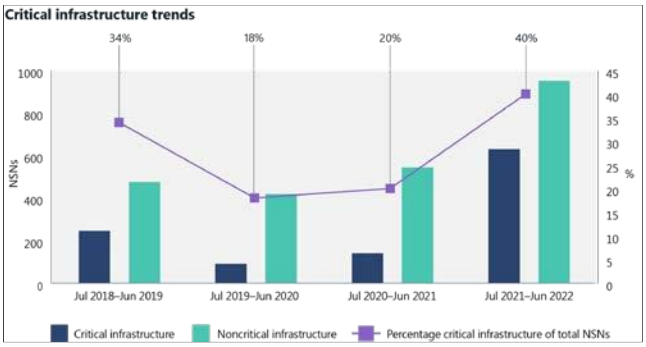

Fig. 1. Attack trend on Critical Infrastructure

Russia is not the only nation state actor involved in cyberattacks. Some other cyber actors such as Iran, China and North Korea have become more aggressive. They employ a wide variety of tactics in order to target the governmental infrastructure, financial and technology companies or to conduct cyberespionage operations across the globe. Their targets span of specific groups of organizations or individuals with a particular focus on IT companies or critical infrastructure. By compromising IT services, the attackers are often able to reach their destination target or to penetrate deeper into the infrastructure. After the IT sector, the most frequently targeted entities were think tanks, academics attached to universities, and government officials.

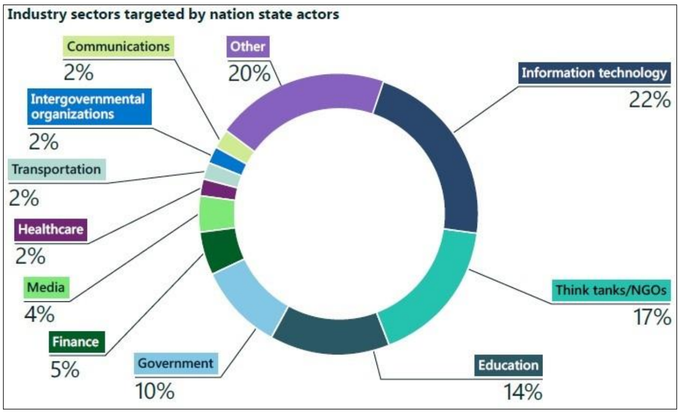

Fig. 2. Targets in industry sectors

### C. *Threats to government's digital infrastructure*

As governments all around the world are concerned about the security of their digital infrastructure, they are increasingly investing in cyber defense capabilities to counter the modern threats. Some governments also invest to support offensive operations and meddle with the technological capabilities of the enemy. A cyber-attack can cause similar damage of a conventional attack and its spectrum is very wide. Due to political developments in the last years, some geopolitical relationships have broken down by signaling much more tense relations in cyberspace. Cyber defense is considered a key challenge for the governments nowadays. Cyber-attacks may have a great impact even on the relations between countries and therefore it is necessary a greater cooperation between nations to share information about threats and attackers incyberspace.

Cyber attackers can use their access and privileges to destroy the data and software on a computer system or networks belonging to governmental institutions and officials. They also exploit possible vulnerabilities such as unpatched software on critical parts of the system in order to penetrate the other parts of the infrastructure. Cyber weapons can be an innocent-looking module or very complex and undetectable software especially those produced by other governments. Often the main goal is to take control of a systemwithout the knowledge of the system's owner, using it for the attacker's purposes whenever they like.

Cyber actors have also increased use of ransomware as a tactic in their attacks. Such tools are developed by the so called criminal ecosystem mainly for financial gains. There are also cases when the attackers conduct just forms of vandalism to damage the system data and deny the access to legitimate users. Cyberattacks using cyber weapons are activities that would classified as crimes in their victim countries.

A particularly troubling issue with cyberattacks is their frequent use of identity deceptions of various kinds which makes tracking and punishment very difficult. It is obviously more difficult to prove responsibility for a cyberattack than for a conventional attack, since it is hard to trace where it came from. The rapid growth of mobile devices and apps, especially smartphones and tablets, are leading to greater chances of cyber threats at workplaces.

## III. Cyberattacks on IT infrastructure of Albanian government

The destructive cyberattacks against the Albanian government IT infrastructure was conducted on July 15 2022. The main target of the attacks was the governmental platform e-Albania which at the time of the attack offered 1225 services to citizens [5]. All services were disrupted and no access was possible for several days. Due to the limited capabilities in expertise, and suspicions that the attack originated from anation state cyber actors, the Microsoft Detection and Response Team (DART) was engaged by the Albanian government to lead an investigation into the attacks [6]. The first and foremost task was to help the government rapidly recover from this cyber-attack. Some other foreign state actors were involved in the investigation of the attacks due to political related reasons revealed by the attackers [7]. According to the findings of DART, the attackers gained access to the network of an Albanian government in May 2021 by exploiting the a vulnerability on an unpatched SharePoint Server administrata.al and fortified access by July 2021 using a misconfigured service account that was a member of the local administrative group.

Evidence gathered during the forensic response indicated that Iran-affiliated actors conducted the attack. This evidence includes, but is not limited to:

- The attackers were observed operating out of Iran
- The attackers responsible for the intrusion and exfiltration of data used tools previously used by other known Iranian attackers.
- The attackers responsible for the intrusion and exfiltration of data targeted other sectors and countries that are consistent with Iranian interests.
- The wiper code was previously used by a known Iranian actor.
- The ransomware was signed by the same digital certificate used to sign other tools used by Iranian actors.

Some other evidences reinforced the confidence that the attackers were acting on behalf of the Iranian government. The main reason was the support of Albanian government for The People's Mujahedin Organization of Iran (MEK), an Iranian dissident group largely based in Albania that seeks to overthrow the Islamic Republic of Iran.

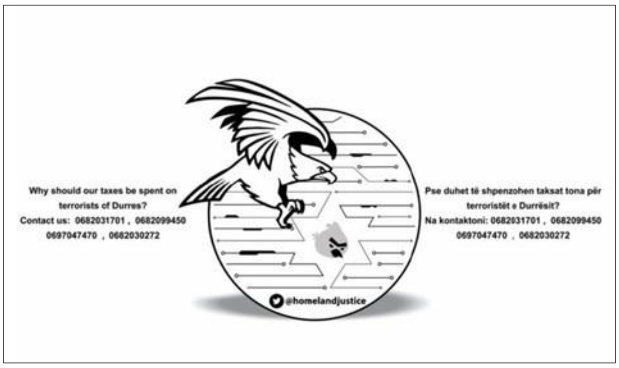
Why should our taxes be spent on terrorists of Durres?
Contact us: 0682031701 , 0682099450 0697047470 , 0682030272
Pse duhet të shpenzohen taksat tona për terroristët e Durrësit?
Na kontaktoni: 0682031701 , 0682099450 0697047470 , 0682030272
@homelandjustice

Fig. 3. The attacker's logo

The attacker's logo is an eagle preying on the symbol of the hacking group 'Predatory Sparrow' inside the Star of David. This signals that the attack on Albania was retaliation for Predatory Sparrow's operations against Iran, which Tehran perceives involved Israel. The message in the ransom image indicates that the MEK, a long-standing adversary of the Iranian regime, was the primary target behind their attack on the Albanian government.

The messaging linked to the attack closely mirrored the messaging used in cyberattacks against Iran which have nothing to do with any institution in Albania. According to [7], the Iranian state cyber actors acquired initial access to the IT infrastructure approximately 14 months before launching the destructive cyber-attack, which included a ransomware-style file encryptor and disk wiping malware. The actors maintained continuous network access for approximately a year, periodically accessing and exfiltrating e-mail content. During that time, they transferred about 20 GB data from the compromised server.

In June 2022, the Iranian hacking group known as HomeLand Justice created a website posting anti-MEK messages. On July 18, 2022, HomeLand Justice claimed credit for the cyber-attack on Albanian government infrastructure and on July 23, 2022, HomeLand Justice posted videos of the cyber-attacks on their website. Initially hosted as homelandjustice.ru, the website was subject of ban within the country. Today it still accessible under the domain name homelandjustice.cx. From late July to mid-August 2022, socialmedia accounts in Telegram associated with HomeLand Justice demonstrated a repeated pattern of advertising Albanian Government information for release.

In September 2022, Iranian cyber actors launched another wave of cyber-attacks against the Government of Albania,using similar Tactics, Techniques and Procedures (TTPs) and malware as the cyber-attacks in July. The main target was the Total Information Management System (TIMS) which is used by Albanian police at border control. TIMS helps automate things like passport checks and cross-referencing people on fugitive databases. The cyber-attack disrupted the TIMS services for several days until the system came gradually back to normal operation.

These malicious actions prompted the government to publicly attribute the July cyber-attacks and to severe diplomatic ties with Iran. Even after this moment, HomeLand Justice continues to publish online sensitive data about the institutions, high ranking officials in administration and individuals. The ban of the social media profiles in Telegram, serving as sources of data leaks, has been impossible so far.

## IV. Analyses of factors and consequences

The main motivation for these attacks was political due to the fact that Albania has allowed about 3,000 members of the Iranian opposition group MEK to settle near Durres, the country's main port.

In the past, the government promoted continuously the online services as a great achievement by integrating thousands of them in one portal named e-Albania. In May 2022, the government had even closed in-person desk services in government offices and mandated the use of digital servicesvia e-Albania. The government portal was used by all Albanians and even foreign residents for a wide range of online public services that were previously provided by desk services.

The Albania's National Agency for InformationSociety (AKSHI) is responsible for the administration and the security issues with considerable financial budget [8]. According to the development strategy, the investments were directed more towards functionality aspects and less to the enhancements of security capabilities. The personnel had standard cyber security trainings to carry not so complex security related tasks. Thus the agency was not prepared toface nation-states actors with unmatched significant offensive capabilities.

The political conflict slowly tuned into cyber conflict paving the way for Iranian state actors to conduct the cyberattacks against the critical infrastructure sectors on 15 July 2022. Because of the severity of the attacks, the Albanian government asked for the support the specialized teams from Microsoft and US security companies. According to the Microsoft Detection and Response Team (DART) report, the attackers gained access in the compromised network a year ago and frequently stole emails throughout 2021, giving them enough time to study the weaknesses and transfer some GB of sensitive and critical data which is being leaked periodically. The factors that led to the success of the attacks can becomplex.

- The government did not focus properly on the security requirements for such critical infrastructure. The growing number of online services was not at the same rate with the improvements and attention to security services. Moreover, the centralized modelimplemented proved to be a single point of failure for the entire infrastructure. AKSHI temporarily shut down public services and all government websites usually accessible via the internet by denying at the same time those services to the citizens. As a consequence, during the attack, the AKSHI inter- dependent network including the website of the Prime Minister's Office, the country's Parliament, and the widely used governmental portal e-Albania was taken down to prevent further damage.
- Lack of cyber security personnel with advanced training to cope with complex and aggressive attacks. The political conflict signaled a growing concern about the use of cyber weapons which required fast and effective countermeasures to deal with possible attacks in the near future. Also the employment policy was not adequate to hire cyber security professionals and experts in the labor market due to the limits in financial support and salaries.
- The centralized management model is vulnerable to aggressive attacks such as Distributed Denials of Service Attacks (DDoS). Without the strong defense capabilities, the critical infrastructures will be threaten continuously and more likely the nation state actors will succeed to violate their availability.
- Security requires continuous monitoring and increasing the awareness of the response team about that is crucial. Negligence in ensuring the security of the critical system can bring big problems. Hence, it is necessary to remain vigilant which was not the case. The attackers exploited a vulnerability to the server unpatched software in order to compromise the entire IT network.

## V. Conclusions

Cyber security is undoubtedly the key focus of the 21st century. The lesson learned from this case is that cyber-attacks are inevitably disruptive and demand greater attention in today's interconnected governmental IT critical systems. The massive attack on Albanian government systems is yet another alarming incident drawing attention to the unprecedented surge in cyber operations sponsored by nation state actors against the public services sector.

With sophisticated and complex security threats in the IT environments posing new set of challenges for governments, organizations and individuals across the globe, there is a need for a high level of alertness. It is obvious that combatingthreats in the cyber space requires tremendous national and international cooperation, coupled with training and awareness as well as taking adequate precautionary actions.

Lack of education and training in the cyber security often escalate the level and intensity of threats. Therefore, governments should appoint cybersecurity specialists for coordinating the nation's cybersecurity policies and activities, initiate a national awareness and education campaign to promote cybersecurity. The government and private industry must work together as this has to be a shared responsibility for preserving the security objectives of critical infrastructure sectors.

## References

[1] https://www.cisa.gov/uscert/ncas/alerts [Accessed on Nov. 17th 2022]

[2] W. Bayles, Network attack. *Parameters, US Army War CollegeQuarterly, 31,* pp.44-58, 2001.

[3] https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022 [Accessed on Nov. 18th 2022]

[4] https://www.cisa.gov/critical-infrastructure-sectors [Accessed on Nov. 18th 2022]

[5] https://e-albania.al/Pages/Statistics/statistika.pdf [Accessed on Nov. 18th 2022]

[6] https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/

[7] https://www.cisa.gov/uscert/sites/default/files/publications/aa22-264a-iranian-cyber-actors-conduct-cyber-operations-against-the-government-of-albania.pdf [Accessed on Nov. 18th 2022]

[8] https://akshi.gov.al