THE 16TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

Management of Cyber-Espionage Intrusions

Mircea Mocanu[1]

Abstract: The soft side of Information War is called either Digital War or Cyber War, and gets larger use worldwide, due to the difficulty of proving the aggression culprit. The defensive posture of the Digital War, cybersecurity, is better developed, at least because everybody needs defense, while less global actors are hostile. However, while the focus is on protection against unexpected destructive actions, digital espionage keeps the victim system running, and uses concealed procedures meant to avoid security measures and continue the illegal exploitation of network data. In cyber-espionage, the objective may be top-secret data, which are strongly protected, but it may also be apparently unimportant customer data, information such as e-mail addresses and credentials. The latter kind, which usually gets less protection, can be later used not for strategic hostile decisions, but for subsequent clandestine operations. Such information becomes of national security relevance for governmental institutions and critical infrastructure facilities. At that level, confidential data are better protected in local servers, but are available to scrutiny by system maintenance software. Therefore, specialized software trusted specifically for system security and technological upgrade can be used by hostile actors for penetrating various wide area networks. Such gateway is the logistic chain of IT companies, whose software products become a force multiplier for cyber-espionage by state organizations or hackers at large. This is the case for the recent SolarWinds cyber-espionage operation, which provides useful insight on clandestine activities, and prompts to the need for improving cyber-security in view of espionage threat. Beyond software solutions meant to strengthen digital system protection, the overall problem requires macro-system solutions leading to better resilience of national information systems. Such requirement surely pushes national security institutions toward improving the organisational architecture of national cyber-security.

Keywords: information war; cyber-security; supply chain; cyber-espionage; SolarWinds; informational systems; hacker; malware; critical infrastructure; GDPR

Specifics of Digital/ Cyber Warfare[2]

The offensive side of Information Warfare has a kinetic component, which means mechanic/physical action, and a subtle/soft component, which occurs in the digital environment. The former means destruction of information infrastructure targeted for aggression, while the latter component implies a cyber-impact on targeted information systems and disruption of their digital program operations.

The soft part of Information Warfare, also called Digital War, or Cyber Warfare, is defined as "a subset of what we call information war, (which) involves non-mechanic attacks on information, information processes, and information infrastructure that compromise, alter, damage, disrupt, or destroy

[1] Danubius University of Galati, Romania, Address: 3 Galati Blvd., 800654 Galati, Romania, Corresponding author: mirceamocanu@univ-danubius.ro.

[2] This first section uses, adapts, and develops paragraphs from Mircea Mocanu, *Intelligence in 21st Century Military Operations*, Bucharest: National Defense University „Carol Ist", 2018, pp. 148-157.

information, and/or delay, confuse, deceive, and disrupt the information processing and decision-making" (David, 1996, p. 10).

Under uncertainties regarding risks and threats, the defensive side of Information Warfare is more advanced, because it requires across-the-board protection of information systems *erga omnes*, either against mechanic attacks, or against cyber-attacks. Physical protection of information systems includes usual measures of critical infrastructure protection, as well as establishing a network architecture able to effectively absorb significant damages inflicted by the enemy, and dispersion of command and control (C2) assets, according to the Network Centric Warfare logic.

The existence of a strategic aggressive capability looming large over the global cyber environment already generates the major risk perceived by the actors in the international security environment. Hence, the efforts to protect information systems against undesired soft actions are more advanced. Among the operational space components, or security environment components in general, the analysts can easily identify hostile international actors who are motivated and capable of executing cyber-attacks the against critical information infrastructure of a country designated as target. But the precise intention, the decision, and the engagement in hostile action are quite difficult to detect early enough for preventing or fending a cyber aggression.

The Information Age generated a variety of *interactions* - the second category of security environment components. There are the actions pertaining to Information Warfare, which unfold after the decision for a hostile cyber action is made. "The threat landscape in coming to be dominated by emerging phenomena such as a customizable modular malicious code and networks of computers being remotely controlled by criminals and used to mount mass denial of service attacks. Targeted attacks on individuals by 'phishing' attacks to divulge personal account details, or on web applications and web browsers, are increasingly becoming the focal point for cybercriminals" (Omand, 2010, p. 71). It is obvious that cyber-threats are operationalized with cyber means: "With malicious cryptography and crypto-virology, armoured viruses that are resistant to counter-measures or mutate to avoid detection, and other dangerous exotica in the cyber-zoo, the offence/ defence race has become all but incomprehensible to the non-expert" (Omand, 2010, p. 72). Naturally, this means that cyber-warfare is over-specialized and high-tech, and its operators must be cyber-experts.

However, for defining a certain threat, warning about a cyber-attack is difficult to achieve, because clear indicators for effective warning systems are scarce, and control on vulnerability parameters is poor. On the other hand, intention of cyber-attack is quite difficult to detect in absence of human source intelligence (HUMINT) acquired from the highest decision level of the adversary organization. In other words, it is almost impossible to catch the culprit with a "smoking keyboard" (David, 1996, p. 4), red handed in cyber-attack.

This difficulty is worsened by the fact that "information strategies", referring to "the recognition and utilization of information and information technologies as an instrument of national power that can be independent of, or complementary to, military presence and operations" (David, 1996, p. 1). Theoretically, cyber-attacks precede the kinetic components of an aggression, precisely aiming to damage the enemy's C2 system, and therefore to maximize the aggression's chances of success.

The specific danger in cyber-attacks lies in threatening "the ability of a nation state's military to interpose itself between its population and 'enemies of the state', thereby causing a loss of sanctuary" (David, 1996, p. 5). Therefore, an important mutation appeared in the information protection philosophy, from limiting and strongly controlling access by compartmentation and information flow restrictions, to

encouraging "the active participation of individuals, communities and companies… to reduce the overall level of risk" (Omand, 2010, p. 73) regarding the integrity of sensitive information. This means a new security culture, adapted to the new battlespace, the new cyber-space/digital space.

Digital warfare can also be approached in the Effects based Operations (EBO) and comprehensive approach logic, by the attack on civilian information systems of strategic importance (for example, banking, energy, health, and transport systems). Such severe hostile actions can cause even economic wars with strategic consequences, as it happened with the attack by North Korea on Sony company, which caused a 100-million-dollar damage, in 2014 (Hughes-Wilson, 2017, p. 431). Also, the Stuxnet virus caused major disruptions in electronic systems of Iran's nuclear installations, in 2014 (Hughes-Wilson, 2017, p. 429), and the NotPetya virus caused huge damage to Maersk Danish shipping company, in June 2017. These kinds of attacks require a multidimensional approach from the intelligence agencies which cannot make an upfront discrimination between a military and a non-military cyber-threat. In fact, in cyber-space, the military or non-military feature of a cyber-attack loses relevance, and the hostile operators are generally called 'hackers'.

At the same time, the chaotic aspect of cyber-attacks can hamper the identification of adversary's intentions, tactics, and capabilities. This feature does not easily reveal useful indications for generating coherent courses of action in cyber-attack damage control. Digital war complexity also points to the combined effect of apparently chaotic attacks: this effect, which is multidimensional and confusing, is much larger than the aggregated impacts of individual attacks (David, 1996, p. 30; 33). The most destructive cyber-war action seems to be the sabotage, "which employs the Denial-of-Service (DoS) type of attack to render useless a network serving certain beneficiaries" (Hughes-Wilson, 2017, p. 426). Such attack occurred in Romania in October 2018, when Constanţa City Hall was cut-off.

Digital Intrusion for Other Purposes than Destruction

A hostile actor, most probably a state or a state sponsored organization, can tamper with information systems of a targeted country for other purposes than disrupting their operation, by either kinetic or soft means. This is the case of espionage, which exploits the targeted information system in view of extracting protected or classified information flowing in that system.

Espionage is not considered aggression. For several reasons, the international community would not work to regulate this activity in behaviour norms and international treaties. Two of these reasons are: first, the espionage is difficult to document at legal standards, except for isolated cases, and second - many countries do it anyway. On the other hand, the combination of these two reasons makes victim governments seek other solutions for such predicament than the usual measures taken in aggression situations. Espionage is often called "the third way" for a reason, right? Nevertheless, in many cases of espionage, victim governments resort to diplomatic actions as retaliation measures. For example, following the conclusions after the SolarWinds hacking operation detected in December 2020, Biden Administration decided, on April 15, 2021, to expel ten Russian diplomats[1]. Shortly, Poland followed suite, in solidarity with the United States, and Moscow responded in kind, after a couple of days.

Among hostile activities, the espionage stands out with its clandestine feature. This means that intelligence actions must unfold in secrecy, "under the radar level", as discrete as possible, for two main reasons: to secure the extraction of as much information as possible, and to protect the operators and their intrusion methods. In cyber-espionage, conspiracy is upheld, and, at the same time, it dovetails the

[1] https://www.nytimes.com/2021/04/16/world/europe/russia-expels-diplomats-sanctions.html.

range of situations considered by risk managers responsible for the integrity of information systems, more precisely, the digital component of information systems.

Another issue of interest is the level of ambition in hostile operations, namely the espionage scope pursued by the hostile actor. Usually, the risk managers are concerned by the most severe possible impact of hostile operations, the effects which are compromising the most valuable data, the top-secret information with the highest importance for national security. This body of information goes to decision-makers at the highest governmental or military level of the hostile state, for major decisions, like surprise aggression, or a strategic political move. However, adversary actors can also pursue their interest to extract data with apparently lower importance in the security environment, with little consequence for the integrity of targeted information systems, for their software operation, or for national security. These data are necessary for planners of future actions of various types, with various other clandestine or operational objectives. In the former situation, the espionage operation has an informative goal, where the prize is valuable information for important decisions, while in the latter case, there is an operational goal, where the prize is data necessary for other hostile actions, albeit clandestine or otherwise. These data do not reach high level decision-makers, they are used by operation planners and agents/hackers.

In its turn, espionage seeking data for operational purpose presents a variety of scenarios and levels of impact. Their description ranges from extracting personal data belonging to a single targeted individual, or data describing a single infrastructure facility, to large-scale operations, which hunt for private data belonging to masses of citizens active in various organizations and domains, governmental or commercial.

Obviously, for low-scale actions, a hacker would penetrate the infrastructure or software of a single informative-operative objective and performs a "sting operation". For large-scale operations, when the hostile actor seeks a massive impact by extracting data belonging to a large population of individuals (either specifically targeted, or randomly harvested), the hacker, or, more likely, the hostile intelligence organization, would not target hardware, but software instead, meaning intrusion into the soft component of the targeted digital system.

For maximum destructive impact, the hackers will not target the software hosted in a certain server, or even operated in a single system/network, but will probably target the mechanism allowing intrusion in numerous such information systems. Therefore, the easiest way is to 'infest' the software products designed to periodically update targeted software carrying or providing access to the necessary protected information. By compromising one of the consecutive versions of update software purchased by macrosystems' administrators, the hackers achieve penetration of numerous targets by the very tools meant to periodically improve the security of those critical digital systems. In a nutshell, the victim itself pays for the poison, and swallows it according to all safety procedures. This logic points to the supply chain operative value, the sensitivity of the logistic architecture meant to update the targeted information system software. This was the case in 2019, when the networks of several American political analysis NGOs were penetrated, and, more recently, the case of espionage operation which targeted the SolarWinds company software products.

Of course, due to the clandestine feature of such actions, prevention efforts are paramount, but warning about a specific hostile action is extremely difficult. Therefore, the most advanced direction of effort against digital hostile operations is *post-mortem* investigation of high-tech nature (in Information Technology - IT). In most cases, such *post factum* activity means the study of hostile *modus operandi* and the impact assessment, in view of damage control management. These activities aim at identifying

the culprit, understand its methods, and identify the vulnerabilities of victim system, which made the intrusion possible, or facilitated the hostile penetration. Of course, relevant conclusions would be used for improving future cyber-protection.

Unfortunately, the post factum investigation in digital environment cannot easily reveal a clear-cut lead from the impact to a certain hostile actor, cannot quickly see all possible consequences, due to the non-linear nature of software processing. Also, the hostile intention variables are not visible to the damage control managers. Given these difficulties, the technological expertise remains crucial, closely followed by intelligence, which "must be a continuous activity. It also means that collection and analysis of information about attacks is vital to maintaining parity with attackers. Finally, it means that defenders must be proactive and undertake efforts designed to anticipate methods of attack so that timely defenses can be developed" (David, 1996, p. 13). The dangerous disadvantage of this asymmetry leads to the conclusion that "the most difficult adversary for an advanced country… would be a society extremely lowly advanced from a technological point of view, with a limited elite of cyber-warriors who would operate from abroad" (Hirst, 2001, p. 80). Such situation also makes a serious challenge for the intelligence agencies, both military and civilian.

In digital environment circumstances, counterintelligence meant to prevent and counter cyber-espionage (penetration on information systems) preserves, though, its human component, but also develops a significant IT component. The new operational space of cyber-protection combines the counterintelligence skills with high engineering expertise necessary for navigation in the digital security realm. The concrete case described below speaks volumes.

Supply Chain Penetration during SolarWinds Espionage Operation

The large-scale espionage operation committed by compromising the SolarWinds company software products was widely presented in the media[1]. Its main issues remain of interest for months in 2021, for its impacts in various angles. The compromised software product, the Orion Platform, with its successive versions, is designed for information network monitoring, maintenance, update, and optimization of host system software in large area IT systems. Such digital macro-systems serve governmental institutions and agencies, or private beneficiaries operating Wide Area Networks (WAN), for example global commercial companies. Orion also oversees the way network resources are utilized and identifies optimization solutions in support of network managers working to overcome current system challenges. The Orion Platform was and still is delivered to a huge number of beneficiaries, both governmental institutions and private companies in the United States and beyond.

To perform its duties, the Orion Platform has access to addresses, passwords, and user authentication procedures. Of course, for a good operation of its own network, each and all beneficiary has all the reasons and interest to update the acquired Orion software, whenever a new version is available.

By using Orion Platform for intrusion, the hostile mastermind installed evil software code lines in packages sent to targeted institutions. In fact, the hackers stored malicious data in genuine files during the usual flow of Orion Platform processing, and thus established hostile presence and 'backdoor' access into the victim system, through the very tool supposed to monitor and secure the protected system. The malware was authenticated and 'signed' as Orion software, then sent to customers and injected into the targeted digital system with SolarWinds security credentials. This way, the customer grants audit level

[1] The following four sections use paragraphs from a series of four articles on SolarWinds 'affair', published in January-February 2021, in www.monitorulapararii.ro.

access privileges to Orion Platform, hence to the hackers, by the malware product called Sunburst. Therefore, the hackers get access to protected data belonging to users and partners of many digital systems, through the compromised Orion Platform version. [1]

This way, the hostile intelligence agency does not directly penetrate the targeted informative facilities, but clandestinely exploits the distribution possibilities offered by the supply chain. Even more, the 'espionage tool' is officially distributed on a large-scale, including to entities that were not intended targets for espionage perhaps, at least not at the beginning. The installation of 'poisonous' tools on the victim is made on victim's cost, and under close supervision for a neat installation procedure.

In the alert[2] issued immediately after the intrusion was detected, on December 17, 2020, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) specifically mentioned, in Overview, that "this adversary has demonstrated an ability to exploit software supply chains and shown significant knowledge of Windows networks. It is likely that the adversary has additional initial access vectors and tactics, techniques and procedures that have not been discovered". Even more, a Microsoft expert declared[3] that using supply chains as intrusion vehicle makes SolarWinds probably the worst cyber event impacting on the United States in many years, because "one of the things that needs to eb off limits is a broad supply chain attack that creates a vulnerability for the world that other forms of traditional espionage do not".

The illegal exploitation of a supply chain software is not new: lately, hackers used more and more this intrusion gateway for achieving either large access to the targeted cyber-space, or destructive power. Intelligence agencies have indeed warned specifically about the danger of this type of intrusion, which leads to most pessimistic consequences in cyber-security.

In the above-mentioned alert, CISA stressed that, after extending its presence and consolidating its integration into Orion, "the adversary creates unauthorized but valid tokens and presents them to services that trust… (such) tokens from the environment. These tokens can then be used to access resources in hosted environments, such as email, for data exfiltration via authorized… (procedures)".

Conspirative Measures Specific to SolarWinds Operation

The conspirative measures are crucial for a successful clandestine operation. For a cyber-espionage operation of SolarWinds scale, achieving success means that hackers must remain 'under the radar level' for months or years, while dodging expensive software protecting its own territory. For that end, hackers, must strike the perfect balance between maintaining conspiracy and reaching their espionage goals.

During SolarWinds intrusions, the hackers proved to be "extremely clever and strategically oriented", they operated accurately and focused, considering long-term objectives, not a sting. According to a FireEye security company report, instead of infiltrating many systems at once, which would have drawn suspicion, the hackers focused on a small number of selected targets, distributed in various networks.[4] Also, using anti-forensic measures, the hackers triggered their own modified Orion functions to process

[1] Feds Race to Turn Off SolarWinds Products Amid Biggest Hack in Years - Defense One.
[2] Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations | CISA/ncas/alerts/aa20-352a.
[3] More Hacking Attacks Found, Officials Warn of Risk to U.S. Government - The New York Times (nytimes.com).
[4] Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor | FireEye Inc.

UserID names, and they used the same UserID format in later actions. Imitations of Orion name patterns are visible in all detected 'backdoor' source codes.

To cover their tracks while exploiting the malware sequence, hackers took care to use only once a computer or an access network for communicating with the injected Sunburst sequence, to avoid a proper attribution. The hackers exploited their malware slowly and stealthy, using long-distance secure 'backdoor' access instead, with genuine passwords stolen from real, legitimate users. Even more, codes were used only once, because security software seek repeatedly used access codes.

Timeline of Initial Shock and Cyber Emergency Response

Regarding the felony of illegal access to software product, the timeline shows the first signals on December 9th, 2020, when a FireEye system supervisor read the alert that somebody had accessed the company virtual private network[1] (VPN) from a new device. Right away, FireEye IT operators started to assess and contain the impact of detected unauthorized access by performing several procedures. Among these, they checked 50,000 code lines for detecting anomalies in the software. At the same time, FireEye notified SolarWinds (the software owner) and Microsoft, and, on December 13th, published the initial investigation results[2] about the intrusion effects.

Shortly, these three IT companies, plus cyber-security compartments in afflicted and suspicioned to be afflicted governmental agencies rushed to respond to the incident, in damage control mode.

In Romania (not identified as possible target in the primary alerts issued in the U.S., the CERT-RO[3] governmental institution initiated necessary investigations for possible SolarWinds-type intrusions in Romanian digital networks[4]. Specifically, CERT-RO[5] started to look for "possible confirmations of the presence of Orion component suspicioned to be compromised by the Supernova 'backdoor' sequence".

In its emergency directive, CISA requested beneficiary entities not to install or reinstall any Orion version before it okays such operation[6]. CISA also requested them to urgently confirm they have cut off their networks within one day plus weekend, to keep them off until further notice, and to report any detected malware.

In addition, SolarWinds issued a set of directions[7] (Advisory), on both Sunburst and Supernova malware, for the beneficiaries, who had to update their networks with the latest Orion Platform 'clean' version, available on the company portal.

IT experts have told everybody which four Orion versions are compromised by malware, and the specific altered code lines were sought for in all computer networks, as were all secondary sequences, generated by Sunburst action. However, after resuming operation with clean Orion versions, all beneficiaries still had to vet all external flow towards any Orion Platform version.

The technical advisory focuses on the detection and elimination of techniques, tactics, and procedures (TTP) used by the hackers to forge the credentials and gain access to resources stored by various victims

[1] A connection from a VPN from a personal computer (PC) running a Windows 10 operating system offers a more secure connection and access to that private network as well as access to Internet. For example, in the case of working from an anonymous place, like a café, a library, or an airport.
[2] U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack | Reuters
[3] CERT – *Computer Emergency Response Team*.
[4] Identificarea serverelor SolarWinds Orion expuse pe internet în spațiul de adrese IP din România (cert.ro)
[5] CERT.RO.
[6] Feds Race to Turn Off SolarWinds Products Amid Biggest Hack in Years - Defense One.
[7] Security Advisory | SolarWinds.

in cloud. These TTPs applied by the 'Trojan horse' already established inside the targeted network by the compromised Orion Platform can be later used for exploiting other vulnerabilities. For diminishing the damage caused by SolarWinds espionage operation, response teams consolidate and monitor the systems that provide both local identification and WAN services.

Primary Observations Regarding the Impact of Digital Intrusion

For cleaning the humongous amount of data in all possibly inflicted networks, absolutely all available data must be checked. This huge volume of bytes is either stored in server memory banks available to headquarters network administrators, or distributed among local branches – also immense, or stored in cloud.

It is also important to point that various entities use various rules for storing maintenance and communication data and protocols appliable to their servers. Therefore, it is possible that information operation logs in various servers no longer contain the necessary records. Thus, in certain cases, information necessary to detect illegal data transfers might be not available, and the trace gets lost regarding user-to-hacker transfers through the malware operated during the usual Orion procedures.

As the hacker's specific objective for each target is not known, the Sisyphean task does not unfold in one attempt, yet is a cumbersome investigation where bland data reflecting months of information flow are thoroughly assessed. Loads of records, protocols, and server–to-user communications are scrutinized at both ends. Most of them are legitimate and have properly utilized the genuine Orion Platform.

Since the intrusion information has been made public, this information can and is being used by other hackers, at least just because they can. The open 'backdoors' are exploited by hackers either as lone wolves or coordinated by hostile countries or crime organizations. This already happened, and the vulnerability is an authentication shortcut allowing remote access to the systems where Orion Platform is installed.

The damage level of networks compromised by Sunburst 'kill sequence' points to a taxonomy on three branches: a) networks where the 'Trojan horse' was installed but never used; b) networks where Sunburst was installed and illegally used, but only limited; c) networks where the malware was installed and intensely used for illegal data extraction. Such taxonomy is certainly useful for developing response measures. However, victim companies should take care to close the detected 'backdoors' even when they are in the first two branches, in order to preclude later hacking actions.

Systematic Treatment of SolarWinds Operation Effects

In support of incident response teams, experts developed[1] long lists of 'indicators of compromise' pointing to hacker's address or network used for communication with the malware. These indications highlight the presence or trace of malware activity in the network under investigation and serve as evidence of cyber-crime, or they reveal the very presence of Sunburst malware. Unfortunately, the list of indicators of compromise cannot be exhaustive, because, in most cases, the hackers used an address or network only once. Therefore, the simple presence of as address is not a solid proof of felony in that network. Even worse, removing a malware sequence does not guarantee that the problem is solved,

[1] How to Understand the Russia Hack Fallout | WIRED.

because the hackers had the chance to install Sunburst in other location of the targeted network. So, during this bone-breaking damage control effort, the hackers can still persist in clandestinely extracting protected information in their SIGINT operation.

The experts even produced a 'kill switch' that eliminates the vicious sequence by taking over the illegal IP addresses and blocking any transfer to and from the hackers, either data or commands.

Another contraption deciphers DNS requests received from the hacker and can be used for understanding the hacker logic in prioritizing targets.[1]

Another IT company suggests a new approach for detecting and preventing illegal actions against security software companies' supply chains. Starting from the simple fact that investigators search for anomalies in protected network operation, experts developed a concept based on tracking the time tags on command and data inputs into the beneficiaries' networks. If these time tags are stamped on the transfer receipts by the action of a monitoring server placed outside the protected system, the hackers will not be able to keep up with the protected time tags, and illegal access anomalies would be immediately detected, not during a post-factum audit[2].

More promising, another concept proposes a software able to equally protect the system developer and the user linked by the security supply chain. This concept is about monitoring a comprehensive image of any cyber-security product by following three issues proved to cause vulnerabilities in the supply chain: intrusion issues, digital signature/authentication issues, and system build quality issues. The monitoring and warning product is designed to be integrated and to permanently accompany the cyber-security software in question, both during its development phase and while its utilization by beneficiaries. This product would constantly detect anomalies and offer guidance for troubleshooting. In this case, anomalies are behaviour differences between successive versions of the respective software. Practically, the monitoring and warning product tracks 'statistical behaviour indicators' that not only reflect, but also predicts the effects to be caused by code sequences actions.

The technological solutions shortly described above refer to software vulnerabilities, but digital systems targeted by cyber espionage also require systemic solutions for diminishing or eliminating vulnerabilities at macro level. For macro-systems, the problem gets new values, where more sophisticated concepts, such as resilience, become of essence for cyber-security.

Vulnerability and Resilience of Digital Systems[3]

When assessing information system vulnerabilities, risk management analysis should start from the Interest served by a Subject (actor in the security environment), because this is the cornerstone of risk management, as Interest is also the key for understanding the idea of Risk as relation between Subject and Danger.[4] Vulnerabilities of a digital system cannot be perceived if the system manager fails to consider an Interest which can be specifically afflicted by a hostile action. For example, the obvious interest of maintaining the system working properly, and uninterrupted. Of course, if the system manager does not take into consideration intrusions that leave the system working, but extract information from the data flow by unauthorized actions, he will certainly oversee any indications that the system is

[1] GitHub - 2igosha/sunburst_dga.
[2] SunBurst: the next level of stealth (reversinglabs.com).
[3] This section uses and develops language from Mircea Mocanu, *O teorie generală a conceptului elementar de risc*, 2018, București: „Carol I" National Defense University, pp 94-98, 150-154.
[4] These terms are presented in Mircea Mocanu, *O teorie generală...*, 2018.

exploited by espionage. Instead, he will proceed only to protect the system from destructive actions, or against minor crime (such as hacking for mercantile objectives: ransomware).

This is where small entities behave differently than large organizations. Usually, small entities disregard the threat of espionage when they do not serve strategic institutions, because unauthorized access to a few personal data is not a catastrophe, especially since the customers take their own security measures. In the case of large organizations though, user data are stored in large quantities, and commercial interests depend on the security of these libraries. The problem of customer data security, or the security of operators within the organization itself becomes crucial for strategic governmental institutions, and for systems serving critical infrastructure (airports, nuclear plants, satellite communications). The reason is that the impact of compromising such data bases can reach the level of national security deserter.

Procedures were adopted in the matter of personal data security (e-mail addresses, identification details, passwords, authentication, and access protocols), and legislation was passed (the GDPR laws). Thus, unauthorized (direct) access to such information is a felony. What is left out is shown by the SolarWinds espionage operation (and other): the integrity of software products meant specifically to protect the integrity of the very networks they are installed in. Here we find the vulnerability to intrusions through the supply chain. The peculiarity of this vulnerability is that a single software product is utilized in several information systems. Therefore, the hostile alteration of such software as Orion Platform can lead to a catastrophic outcome, exactly on the principle of EBO. Detecting such vulnerability is less probable in the case of a single beneficiary entity that focuses on protecting its own data, counting on the highest security of contracted cyber security software.

In the military, Vulnerability can be defined as "the weak, sensitive point of someone or somewhat, pertaining to its own system, coming from within, while the threat, danger, and risk are external to the system in question, the system they influence" (Nicuț et. alia 2011, pp. 170-171). This definition includes a comparative explanation, while the dictionary definition is just general. The definition in the military is relevant for the cyber espionage threat because the danger operates in the national security domain.

Vulnerabilities display a wide range. For digital systems, although the problem dwells within a single operational field and the digital environment, the diversity continues, due to the complexity of this new realm of human activity. On the other hand, vulnerabilities are difficult to define for consequences of cyber espionage, because the impact is difficult to measure.

In SWAT analysis, vulnerabilities are tenants of the Weaknesses quarters, but vulnerability analysis can be conducted also for Strengths, depending on the objective, or the phase of risk management planning. For information systems and the threat of espionage, analysis elements must be identified keeping in mind/starting from the Security Interest in sight. This approach leads to various lines of though and courses of action to be considered, depending on the system's dimensions and security value.

Studying vulnerabilities is of paramount importance for risk management and for strengthening the Subject's capability to cope with Danger, generally speaking. This "ability to recover quickly from illness, change, or misfortune" (Universal Dictionary, 1987, p. 1303) is called resilience. For systems, the World Economic Forum defines resilience as the ability "to reorganize in conditions of change, and to secure continued operation of its core functions despite the impact of risks generated externally or internally" [1].

[1] *** http://www3.weforum.org/docs/WEF_Global Risks_Report_2011.pdf, p. 42.

For "building resilience in view of coping with unknown risks, governments or commercial companies should use business continuity planning, secure resource stocks, relax tensions in the system, or diversify core supply sources"[1]. However, coping with espionage requires an additional set of skills, because spies are interested to keep the system running. In case of espionage by penetrating the supply chain, the problem of resilience must be considered at high level, for macro-systems, because this is where consequences can be understood and identified. At macro level, resilience leads to diminishing sub-system vulnerabilities to intrusion by compromising software products which are not subject of scrutiny by the sub-system managers, being considered safe by supplier responsibility. Therefore, resilience appears to depend on flawed assumptions regarding system interactions with other sub-systems assumed to be safe. Obviously, solutions lead to macro level management, but also sub-system managers may check their assumptions when analysing system vulnerabilities as part of cyber-risk management.

Crossing from the macro level of large information systems to the macro level of organizations responsible for cyber-security, recent digital environment events suggest institutional measures which have already been initiated and will certainly develop. They are planned in most countries and in NATO, for consolidating the institutions responsible for this strategic domain, as well as commercial companies.

Conclusions

Considering the dimension of its impact on governmental and industrial/critical infrastructure networks in the United States and other countries, SolarWinds espionage operation is a major cyber-security event of the nature described as communication espionage (COMINT – *COMmunication INTelligence*), part of electronic signals espionage (SIGINT – *SIGnals INTelligene*).

Hackers' audacity dwells not in the strategic level of their targets, but in the choice of penetrating the supply chain software, the very instrument of monitoring the networks and balancing – authentication of network communications with legitimate customers. It is also important that the culprits did not target top secret information, strategic importance servers or top-secret data bases. Also, beyond primary estimations, it is not known for sure what information was extracted. These specifics reflect the espionage operation planner cunning and causes a high degree of difficulty for countering the intrusion effects. It was underlined that, once the hackers gained access through the backdoor of strategic networks, "they have the ability to sit there, slurp up all the traffic, analyze it. We need to be paying close attention to what else are these actors looking for. Where else may they be? Where else may they be lurking? If they've got access, they're not giving it up easily"[2].

An expert has concluded that "we've always known that these types of attacks were possible, and in fact, we have seen them elsewhere, such as in Ukraine with NotPetya. So, it was not at all surprising that this took place. It was surprising that the Russians were this successful for this long, without being detected. I think the U.S. govt, and frankly, the entire cybersecurity industry needs to have a lot of introspection and reflection on the massive failure that's occurred here. And again, this absolutely needs to serve as a wake-up call to all of us"[3]. This point of view underlines the general principle in security, that, if something is estimated it was possibly stolen, it is better off to pursue the hypothesis that the spy objective has been achieved.

[1] *** http://www3.weforum.org/docs/WEF_Global Risks_Report_2006.pdf, p. 6.
[2] How Russian hackers infiltrated the US government for months without being spotted | MIT Technology Review.
[3] https://www.thecipherbrief.com/column_article/the-russians-have-issued-a-wake-up-call.

In its December 2020 directive, CISA concluded that removing the guilty code lines from compromised software would be extremely complex and challenging for victim organisations. Healing will be difficult and long and recovery spells measures of a different nature, beyond technical investigations and response actions seen in the aftermath of SolarWinds espionage operation. Cyber Warfare is the most dangerous facet of hybrid threats, considering the gap between the possible huge impact and the meagre possibilities to prevent a massive cyber intrusion or attack, in absence of an international regulation designed to limit this form of hostile activity.

References

*** (1987). *Universal Dictionary*, London, New York, Sydney, Cape Town, Montreal: Reader's Digest Association Ltd.

*** http://www3.weforum.org/docs/WEF_Global Risks_Report_2006.pdf.

*** http://www3.weforum.org/docs/WEF_Global Risks_Report_2011.pdf.

Alberts, David S. (1996). *Defensive Information Warfare*, Washington D.C.: NDU Press, Institute for National Strategic Studies, National Defense University.

Hirst, Paul (2001). *Război şi putere în secolul 21. Statul, conflictul militar şi sistemul international/ War and power in the 21st century. The state, the military conflict and the international system.* Filipeştii de Târg: Ed. Antet XX Press.

Hughes-Wilson, John (2017). *Serviciile secrete/ Secret services*. Bucharest: Ed. Meteor.

Mocanu, Mircea (2018). *Intelligence in 21st Century Military Operations/Intelligence în operațiile militare ale secolului XXI*. 2nd Ed. Bucharest: National Defense University „Carol the I[st]".

Mocanu, Mircea (2018). *O teorie generală a conceptului elementar de risc/ A general theory of the elementary concept of risk.* Bucharest: Ed. Universității Naționale de Apărare „Carol I".

Nicuț, Valeriu *et alia* (2011). *Operation Planning Handbook*/*Manualul de planificare a operațiilor*. Bucharest: Ministerul Apărării Naționale.

Omand, David (2010). *Securing the State*. London: Hurst and Co.

Internet Resources

Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations | CISA/ncas/alerts/aa20-352a.

CERT.RO.

Feds Race to Turn Off SolarWinds Products Amid Biggest Hack in Years - Defense One.

GitHub - 2igosha/sunburst_dga.

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | FireEye Inc.

How to Understand the Russia Hack Fallout | WIRED.

How Russian hackers infiltrated the US government for months without being spotted | MIT Technology Review.

Identificarea serverelor SolarWinds Orion expuse pe internet în spațiul de adrese IP din România (cert.ro)/Identification of SolarWinds Orion servers exposed on the Internet in the IP address space in Romania (cert.ro).

www.monitorulapararii.ro.

More Hacking Attacks Found, Officials Warn of Risk to U.S. Government - The New York Times (nytimes.com).

https://www.nytimes.com/2021/04/16/world/europe/russia-expels-diplomats-sanctions.html.

Security Advisory | SolarWinds.

SunBurst: the next level of stealth (reversinglabs.com).

https://www.thecipherbrief.com/column_article/the-russians-have-issued-a-wake-up-call.

U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack | Reuters.