Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 - print, 2545-0719 - online
2018, Volume 50, Number 3(189), Pages 57-71
DOI: 10.5604/01.3001.0012.6227

Original article

Advanced persistent threats as a manifestation of states' military activity in cyber space

Boguslaw Olszewski

Institute of International Studies, University of Wrocław, Poland,
bogusław.olszewski@uni.wroc.pl

INFORMATIONS

Article history:

Submited: 12 November 2017

Accepted: 21 May 2018

Published: 30 September 2018

ABSTRACT

The term Advanced Persistent Threats (APT, APTs) has a relatively short history – originated in the United States' government spheres and as such was referred to cyber attacks waged by a state actor. The emergence of such threats has been linked to the evolution of the hacker underground that took place after 2000. The activity of specialists swelling the Black Hat ranks had the nature of criminal offences, targeting data collected by corporations and state institutions. Despite a dozen or so years of experience with APTs, they continue to be a dynamic category of contemporary cyber security threats, with many evolving components beyond simple classification. Their unambiguous identification as a strictly separate type is obstructed mainly by the complex structure of such attacks, prompting analysts to locate them in a catalog containing various known vulnerabilities, mechanisms, cycles and variables.

The analysis of the problem and the evolution of attacks to date has led to the hypothesis that Advanced Persistent Threats are now in the phase of their further modification and testing as a means of offensive action in inter-state and asymmetric conflicts. Armed forces and special services of states saw in them not only a tool per se to achieve economic and military advantage, but a theoretical basis for further research on the development of advanced cyber weapon.

KEYWORDS

APT, cyber warfare, cyber weapon, state

Introduction

Advanced Persistent Threats (APTs) are classified as new types of cyber security threats. Introduction of this term is attributed to the United States Air Force (2006), and its broad dissemination to the analytical centers dealing with this issue, including the Mandiant (FireEye) IT security-consulting services. In public space this term appeared in 2009/2010, which is the first incident widely reported in the media. Since then, many analyzes have been carried out both on the grounds of IT security and

broadly understood international cyber security. This means: "the emergence of heavily geared, long-term, international espionage and sabotage campaigns conducted by secret public actors is the most significant new element in the threat landscape" [Advanced Persistent Threats… 2011]. As a consequence, the US authorities themselves have been identified as a source of APT: "viewing data by the government is potentially «advanced persistent threat», in addition to sophisticated malware and cyber attacks" [Smith 2013].

A broad number of definitions of *Advanced Persistent Threats* have been recognized so far, however the main feature reflecting the essence of the problem has been preserved in all of them. The Estonian Cooperative Cyber Defence Center of Excellence (CCDCOE) proposes three approaches from the point of view of the theory of the United States. The first is a modified version of the definition contained in the NIST document, which treats APT as "an opponent with a sophisticated level of specialized skills and significant resources, which allow for achieving the set goals by using multi-vector attacks (e.g. cyber, physical attacks and deception). Typically, the goals comprise the establishment and extension of points of reference in IT infrastructure of target organization, with the intention to extract information, undermine or hamper critical aspects of a mission, program or organization, and establish them for the achievement of these goals in the future (…)" [Kissel 2013]. The second approach, from the point of view of the Department of Homeland Security (DHS), incorporates the initial part of the modified NIST definition. In the third one, the CCDCOE publishes the state-centric formulation by the Democrats' advisory body in the US Senate, according to which it is "a group, such as a foreign government, with both the ability and intents to continually and effectively target a specific subject often for spy operations or an attack" [Cyber Definitions n.d.]. In turn, the U.S. Air Force defined APT as "complex cyber attacks on specific purposes conducted over a long period of time" [APT: The Best Defense… 2014, p. 2]. They are also referred to as "contemporary, automated versions of traditional espionage, which originally involved people working in the physical world" [Cyber Espionage… 2011, p. 3]. They are also described as "used by governments to destroy data and steal the most accurate state and commercial secrets" [APT: The Best Defense… 2014, p. 3]. Further, the editor-in-chief of the Data Insider blog, Nate Lord, summarizes them as "an attack where an unauthorized user accesses a system or network and remains undetected there for a long time" [Lord 2018]. While, "advanced long-term attacks" [Bequerel 2013] or "advanced persistent threats" are among the Polish translations of the term [APT: Zaawansowane… n.d.].

As can be seen from the above, APTs are a specific conglomerate of activities aimed at delivering precisely defined tasks (e.g. theft of classified data) usually undertaken by teams of high-level specialists. They are not limited to a single attack, but are a sequence of their wide variety – from the most common and possible to execute through *script kiddies* to unrecognized, exploiting an unknown wide vulnerabilities and technology. They belong to the new generation of cyber threats, involving mostly state actors and crime groups acting autonomously or on behalf of the former, using multi-vector attacks with a variety of tools, remaining undetected for a relatively long time. Their purpose is primarily organizations and businesses, and especially their data re-

sources that enable effective functioning in a knowledge-based economy. These may be innovative solutions, innovative technological processes under development or widely understood intellectual property. They are characterized by the use and search for advanced technologies – hence they are addressed to entities in the armaments sector or governmental administration. The APT attacks, therefore, concern individual (citizens) and collective (enterprises and corporations) targets, and eventually state governments.

1. Overview of former incidents

At the outset, it should be noted that even in the case of APTs disclosure, they belong to the overwhelming majority of closely guarded secrets of affected entities, which is in their broad interest, especially if these are military or governmental targets. However, they most often remain undetected, as both the CEO's and the IT security staff is frequently unaware that they have become victims and, in principle, underestimate negative effects of a potential attack. The following examples of detected *Advanced Persistent Threats* are widely known to the public not only because of the high business profile of victims and the volitional disclosure of those events, but also due to the evidence provided by third parties, which, according to the Verizon report, is expected to contribute to about 90% of APT detection [2012 Data Breach… 2012, p. 3]. They have become the main source of knowledge about this phenomenon and model case studies analyzed by cyber security professionals. The examples below are only exceptions to the entire APT collection, which are exhaustively described in the reports available on the Web, as well as presented in a summary form, among others, on the KasperskyLab website (Targeted Cyber Attacks Logbook).

The operation discovered by Clifford Stoll from the Lawrence Berkeley National Laboratory in the late 1980s, described in detail in his book, is one of the first widely known examples of APTs [Stoll 1989]. Markus Hess, a student at the University of the Federal Republic of Germany, kept materials relating to the American Star Wars military program under surveillance on the order of the Soviet KGB. Starting from 1985, he penetrated network resources of a Californian college using satellite broadband. Stoll uncovered this activity a year later on the basis of minor financial inaccuracy (75 cents) in the Unix database and created a *honeypot*, which allowed him to locate and arrest the hacker along with his four co-workers (Karl Koch, Hans Huebner, Peter Carl, Dirk Bresinsky), coming from Hamburg, West Berlin and Hannover. Using ATA they obtained access to thirty computers possessed by the U.S. Army and external contractors, among others, the Optimus database in the Department of Defense, computers belonging to the Jet Propulsion Laboratory in Pasadena and laboratories in Los Alamos and Argonne. Moreover, the hackers (in exchange for money and cocaine) transferred sensitive data obtained in Japan, France, Britain, Switzerland and Italy to the KGB.

American military installations were attacked at the turn of the 20th and 21st centuries (1999) when the APT was detected. Known as the Moonlight Maze it had been conducted for two years against the US Department of Energy, NASA and the Pentagon.

Thousands of files were then transferred, including maps of military installations and information regarding *hardware*, all of this with the use of the Russian *proxy* server.

The series of APT attacks, particularly intense in the period from November 2004 to December 2005, originating from the Chinese province of Guangdong, targeted at NASA, Lockheed Martin, Sandia National Laboratories and Redstone Arsenal, is the most well-known activity run on the military ground. This wrote the history under the name *Titan Rain*, and during this time the Global Information Grid Network being under the jurisdiction of the US Department of Defense was scanned more than 3 million times a day. During this four-year operation, the most affected sectors included aviation, defense, financial, energy, pharmaceutical and advanced technologies. The British Foreign and Commonwealth Office, the US Defense Information Systems Agency (DISA), the Naval Ocean Systems Center in San Diego and the U.S. Army Space and Strategic Defense in Huntsville were infiltrated. Military objectives were taken over within a few hours, however, due to the isolation of military subnets containing classified and secret information (SIPRNet), the inflicted damage was reduced to obtaining data on technological and industrial processes.

The attack on the US fuel sector in 2008, which affected three companies: ExxonMobile, Marathon Oil and ConocoPhillips, is an example of *Advanced Persistent Threat* related to industrial espionage. Corporate executives were completely unaware of this fact, and it was not until the Federal Bureau of Investigation (FBI) notified them. Although it was not possible to precisely determine the source of activity, "the flow of certain data from the oil company's computer to a computer in China" was uncovered [Clayton 2010]. It was a fragment or prelude to a broader operation known as the Night Dragon, targeting the global fuel and energy sector, which began in November 2009, with victims such as ExxonMobile, Shell and BP, as well as decision makers in Kazakhstan, Greece, Taiwan and the USA. The vulnerability of Microsoft Windows was exploited, and the data lost mainly concerned financial projects and operations; the Command & Control (C&C) server was located in Heze, in the Chinese province of Shantung.

In 2009, the SecDev Group published a report on another APT, known as GhostNet, the activity sourced from the Chinese island of Hainan (though US and Russian intelligence agencies were also suspected). Intruders targeted Tibet, using four C&C servers and a network of "1,295 infected computers in 103 countries" [Tracking GhostNet… 2009, p. 2]. These included the Dalai Lama's private office, information resources of the Tibetan government in exile and NGOs data, which were explored in real time with the "gh0st RAT" Trojan horse to take complete control over workstations, including their cameras and microphones. What is more, embassies of several countries, including India, Pakistan, Portugal, Romania and Germany, as well as foreign ministries (Iran, Philippines, Latvia, Indonesia, Barbados etc.), which additionally became part of the bot network, were among the targets.

The Aurora operation is the first widely discussed APT and "it is believed that it targeted 34 organizations" [Tankard 2011, p. 16] (including Juniper Networks, Adobe Systems, Google, Yahoo!, Symantec, Northrop Grumman, Morgan Stanley, Rackspace and

Dow Chemical). Google reported it in January 2010, however it probably "had started about six months before" [Tankard 2011, p. 16]. The attack was performed using the *zero-day* vulnerabilities (CVE-2010-0249) detected in Internet Explorer and the Trojan horse Hydraq downloaded from the infected Web site. The vast majority of discredited companies and organizations associated with industries such as state defense, armaments, electronic equipment and aeronautics preferred to remain anonymous, especially since, according to McAfee, the main goal was to modify the source code repositories. "Sophisticated tactics that were not previously encountered outside the defense sector" [Ghafir and Prenosil 2014, s. 2] were used, including many types of *malware* – the APTs were carried out via the Elderwood platform, and the traces left behind once again led to Chinese hackers. The fact that APT also covered the Gmail accounts of Chinese human rights defenders is the additional evidence incriminating the People's Republic of China. APT1, RSA, Stuxnet (although some analysts disagree to grant Stuxnet the APT status [Cloppert 2011], Shady RAT, Duqu, Flame, and Red October are further examples of the ATPs.

2. Military application of apt

The current trend is to continue the application of APT for political and, in particular, for military purposes, despite the common opinion suggesting their original character according to which "APT was once the domain of nation states" [APTs. New waves… 2015, p. 3] and currently has supposedly lost significance. This in no way means eliminating this source of sophisticated long-term threats, but rather shifting emphasis and focusing attention on APT's more spectacular media impact on commercial players, especially giants such as Google and Sony, since greater emotions are generated by information about personal data leakage than, for instance, a theft of constructional secrets of new weapons, the more that the latter do not quickly appear in public space. The APT evolution cycle covers the late 1990s (military objectives), 2000-2004 (non-military government targets), 2005-2009 (defense industry) and 2009 to date (intellectual property and software development companies). Thus, "considered traditionally as state-sponsored activities and targeted at government networks, threats have also become problematic for businesses" [Advanced Persistent Threats Awareness 2013, p. 6] only for a decade.

The technological race in the field of defense causes that attacks by cyber armed forces and cybercriminals hired by governments are constantly aimed at contractors – especially of the most technologically advanced army of the world, i.e. the U.S. Army (Lockheed Martin, Boeing, Raytheon, Northrop Grumman), but also at the rest of the 100 leading military sector subcontractors. State actors themselves bear the risk adequately to the saturation of their social fabric with IT, the advancement of their ICT infrastructure and their impact on the regional and global economy. What is more, due to a role played in the international arena in the context of cyber security, Estonia remains at the forefront of threatened countries (also because of the location of the NATO Cooperative Cyber Defense Center of Excellence). Close inter-sectoral coopera-

tion causes that "cyber attacks are a new front for continuous warfare between states, criminal organizations and commercial companies" [Gajewski 2013].

The further development of the above-mentioned direction of APT operations is reflected in the use and creation of new structural vulnerabilities. This is about the widespread exploitation of hardware gaps, often at the production stage. *Hardware* vulnerabilities are complementary to software; in the case of microprocessors: "some manufacturers deliberately leave an access gap for post-production testing purposes. A manufacturer usually keeps information about test protocols secret, but if attackers learn how to use this interface they will gain access to the code" [Skorobogatov 2005, p. 28]. A similar tendency is evident on grounds of internal security – the National Security Agency (NSA) places *backdoor* on equipment from companies such as "Cisco, Dell, Western Digital, Seagate, Maxtor and Samsung" [Farber 2013]. *Hardware* in the form of a USB flash drive was used in Stuxnet (although it has the discussed APT status, it was necessary to undertake preliminary actions of such nature in order to perform it) and Gauss (detected in 2012) attacks.

Hence, *Advanced Persistent Threats* are embedded in the wider context of cyber warfare and offensive activities conducted by means of network tools. The fuzzy nature of cyber military operations and the lack of uniform solutions under martial law (apart from the attempt to codify cyber armed operations based on the well known international law in the form of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*) and public law make them extremely difficult to be finally classified. All the more so since adopting a radical perspective means an open international conflict. Hence, numerous APTs of cyber attack nature end up being given a label of cyber espionage, or are said to be "one of the most dangerous cyber criminal activities" [Bequerel 2013] and as such are left by default in jurisdictions of states applying their criminal codes towards attackers.

The origins of *Advanced Persistent Threats* are therefore related to the military sector, and now, "originally used to describe cyber intrusions against military organizations, APT has evolved and is no longer confined to the military" [Chen et al. n.d.]. This does not automatically mean that the number of *Advanced Persistent Threats* aimed at the military sector is decreasing, but merely indicates the extension of the target catalog with commercial entities – in particular with regard to institutions and companies that cooperate with the military under contracts or research and development activities. It is worth recalling that the so-called *kill chain*, described by Admiral Jonathan Greenert and General Mark Welsh in the article in "Foreign Policy" (May 17, 2013) was the starting point for describing the APT's "life cycle" [Greenert and Welsh 2013]. Several dozen of exemplary APTs presented in "Chronicles of Targeted Cyber Attacks" by KasperskyLab have the status of military action. These include: Naikon (discovered in 2011); CosmicDuke, MiniDuke, NetTraveler, Machete, Red October, Icefog (2013); Animal Farm, Dark Hotel, Turla, EpicTurla, Sofacial, Equation, Desert Falcons (2014). Some of them under the names of *malwares* used during attacks, which results from the fact that APTs are often associated with "highly sophisticated malware" [Virvilis et al. 2013, p. 396].

The distributed nature of the APT comprises both military objectives and the civilian defense industry realizing orders for the defense sector. The impact of the loss of sensitive intelligence or strategic data on national security is undisputed, and "APT cyber attacks have become very convenient and effective tools for infiltration of foreign defense systems or theft of military secrets, primarily due to the relative ease of their execution (compared to traditional spy methods) as well as a low risk of revealing the actual source and beneficiary of such an attack" [Gajewski 2013]. Although almost every state has been working on achieving cyber combat capabilities, the United States, the People's Republic of China, the Russian Federation, Pakistan and Israel are among the main players in APT application for military purposes. As far as ATP is concerned, the first three, especially the oppositions: China – the USA and the USA – the Russian Federation are the most prominent. Particular groups behind APT have their own numbers upon the FireEye notification: APT28 refers to the Russian Federation, APT1 and APT30 to the People's Republic of China. The case of APT1 activity is a model example of the *Advanced Persistent Threat* application. In 2010 the Californian consultancy company Mandate FireEye dealing with advanced cyber security threats (especially APT) issued the report entirely devoted to APT1 in which it was underlined that there was no way to determine the scope of the Chinese authorities' involvement [Mandiant M-Trends… 2010, p. 1]. However, three years later, such evidence was provided in the subsequent report titled *APT1 Exposing One of China's Cyber Espionage Units*.

Under the aforementioned development, a Chinese unit known as U61398 operating from a building on Datong Road 208 in Shanghai was involved in such activity since at least 2006. The group leased a fiber optic line from China Telecom. 141 entities became its victims; APTs were conducted against 91 of them throughout a year, while the record period of time devoted to one organization was four years and ten months. The record-breaking data outflow from one entity reached 6.5 TB, and 937 C&C servers used by U61398 were indicated in the reporting year. Another such case is APT Naikon, which is most likely part of the People's Army of China as the U78020 unit. Similar actions come as no surprise in view of the fact that colonels of the People's Army of China raised the issue of strategic use of cyber weapons in the book titled *Unlimited Warfare* in 1999 [Liang and Xiangsui 1999, p. 25; APT: The Best Defense… 2014]. The threat from China is so significant from the US point of view that the Congress devoted a report to it: *Report to the Congress of the U.S.-China Economic and Security Review* Commission [2009 Report to Congress… 2009]. After the attack on the Global Information Grid in 2006 Major General William Lord admitted: "China has downloaded 10 to 20 terabytes of data from NIPRnet" [Carvey 2006].

In 2008, the Department of Defense reported 54,000.640 cyber incidents and predicted further 87,570 in 2009 [2009 Report to Congress… 2009, p. 168]. *Advanced Persistent Threats* from the PRC are not limited to purely network activities and show growth trends. In 2010 the U.S. Navy purchased over 59 thousand microprocessors intended for installation in its devices. Ultimately, it was found that they were counterfeited in China and "could have been hacked" [Rawnsley 2011]. In view of the above, offensive cyber attacks are emerging in the context of assessing progress in China's

strategic capabilities. The following classification places APTs as precision cyber weapons, comparable to kinetic smart bombs.

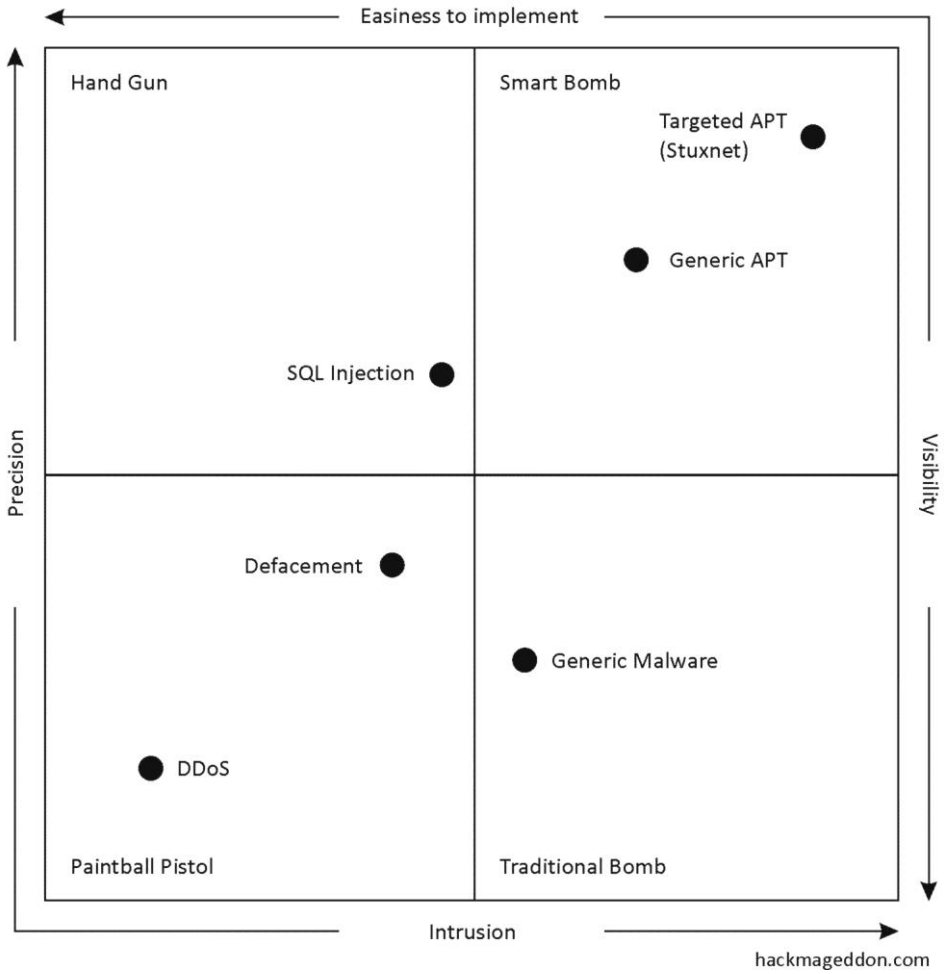

Fig. 1. Classification of cyber weapons
Source: [Based on: Passeri 2012].

A similar situation is encountered between the USA and the Russian Federation, as evidenced, for example, by the case of Agent.btz, which began in 2007 and "infiltrated local networks of the US military operation in the Middle East in 2008" [Gostev 2014]. Then the Pentagon issued a statement in which the Russian Federation was accused of attacking U.S. Central Command computers (by the way, this was not the only attack on headquarters responsible for Iraqi and Afghanistan operations – in 2015 hackers linked to the so-called Islamic State attacked its Twitter account, where they disclosed, inter alia, strategic simulations of the US-China conflict (this type of activity is not classified as APT), including at least one "highly protected classified network" [Barnes 2008]. Another example is APT28 activity: "Tips in malware from APT28 suggest that the group consists of Russian speaking people operating during working hours in the largest cities of Russia" [APT28: A Window Into… 2014]. The popular tactic of spear phishing was used during the course of *Advanced Persistent Threats* called Black Ener-

gy accompanying the military action in Ukraine, which targeted the energy sector of this country.

Indirect attacks on military infrastructure are carried out with respect to contractors who, as non-military business organizations, ultimately decide on their inclusion into the category of operations against civilian targets. In fact, they are aimed at the armed forces of states, seeking to weaken them and gain military advantage by stealing data and identifying network defense systems. Lockheed Martin was the victim of the APT targeted at stealing information about the F-35 fighter, which resulted in the appearance of its Chinese clone under the name J-31. It is possible to anticipate further attempts to surveil this contractor, especially given that it has conducted research on the military aspects of cyber space. As well as Raytheon that is not only a recipient of US defense orders, but has been pursuing a broad strategy related to cyber security on a global scale, which is reflected by the cooperation with the Estonian government launched in March 2015 and implemented in the field of its national cyber security. For this reason, corporations cooperating with armed forces take an active part in fighting APT.

The success of APT in military terms is further compounded by the inconsistent categorization of attacks themselves. These operations serve as a means to explore the military infrastructure and estimate the impact force of an enemy. As such, they are hostile acts in the digital environment, bearing attributes of offensive weapons, negatively impacting defense capabilities of a target state. It can therefore be assumed that "in recent years APTs have proved to be the preferred cyber weapons for larger, more sophisticated attackers" [APT: The Best Defense… 2014, p. 3]. However, classifying them as acts of espionage allows for avoiding an open kinetic military confrontation, inevitable in the case of identifying APTs as offensive activities. Hence, they are labeled in a way to avoid the escalation of interstate conflicts, which furthermore enables them to improve cyber attacks and cyber defense methods in real-world conditions. Their popularity stems from the fact that acts when cyber weapon is used "can significantly weaken the morale of the army and its capability, and even the desire to conduct effective countermeasures" [Kostecki 2012, p. 62].

3. APT and global safety – perspectives

Both superpowers and smaller state entities compete not only for the strongest position in the global power system, but they also claim to be the most advanced in the field of high technology (especially teleinformatics) that shape the lives of modern societies, constitute a representative proof of the advanced level of economic, scientific and military development. Belonging to the elite club for the most technologically advanced countries is also manifested in the impact on the current situation in cyber space, which is *de facto* related to establishing influence zones as well as control over network resources. Governments that seek to maintain their status use their potential to develop methods for supporting these efforts as regards IT, and then apply them in informal negative transactions of cyber crime or cyber espionage nature. Due to the fact that the military sector is a priority and therefore most funds are pumped into it,

especially its research units, the need to develop operational capabilities in the digitized battlefield takes the form of combat use of IT achievements. *Advanced Persistent Threats* are ideally suited in this field, coupled with the process of creating global geopolitics. The evolution of cyber threats (including APT) has made cyber space officially recognized by NATO as a field of combat operations, its training center has been holding annual cyber security training for years, and other state cyber strategies and national centers supporting military efforts in this field have been established. In view of the fact that the military sector is one of the most financed structural elements of a state, it is very likely that APT groups are most frequently created within armed forces and they remain secret, as well as effects of their actions, thereby occurrences of purely military targets are extremely rare in public statistics (if not related to contractors or government targets).

Repeatedly, governments routinely hire or sponsor groups of cyber criminals in order to hide their own (political, military, or economic) motives for illegal cyber activity – for example, the Russian Business Network group operates in the Russian Federation with the approval of the FSB. Moreover, states aspiring to take the best positions in the evolving power shifts but lacking the resources of knowledge move to illegal activities, take advantage of financial resources and to a greater extent use APT *outsourcing.* When a government entity does not have the right resources, it can hire hackers to accomplish goals set and have them develop programming tools to enable APT or involve teams of programmers already possessing such software. It can also pass on previously developed tools and order their further modification and carrying out an attack to divert any suspicions from itself. Therefore, alternative APT definitions appear, understood in this context as "attacks on a state" [Andress and Winterfeld 2014, p. 28], with references made to "state-controlled or sponsored groups" [Andress and Winterfeld 2014, p. 30].

APTs constituted by forces at the disposal of a state actor are not the only source of danger. A separate problem is the involvement of ideologically motivated individuals or groups that do not act on government orders and do not expect financial gain, but attack in the act of contesting the established reality. The execution of orders for non-state actors (terrorists, partisans, drug cartels, etc.) is yet another example. Organized criminal groups lacking adequate technical and intellectual capabilities may be assigned the role of intermediaries acting on behalf of any entity, ordering an attack to known hacker groups, thus constituting another element (layer) that obscures the image of a given APT. In view of the anticipated future evolution of APT, new technology platforms appear that enable the new-generation protection: "IT security experts and analytical companies predict that threats of this type will continue to grow and enterprises will need to redefine security rules to protect their infrastructure from new attacks so as to cover pro-active protection against these threats" [Trend Micro Deep… n.d.]. The unified security control, context-awareness and intelligence are anticipated to play the essential role. All these factors make that "a cyber conflict is becoming ubiquitous, though unnoticeable for many" [Harrel 2015, p. 9]. Since "almost infinite variations of strategies against APT" exist [APT: The Best Defense… 2014, p. 7], the supply in the hardware and software security market is increasing, and the spread of

knowledge about this phenomenon will result in its further mutation towards the next APT generation.

Conclusion

Becoming a target of APT does not automatically mean that a hostile state apparatus and its armed forces are behind the attack. In many cases, these are rather competitive companies ordering APT to gain market advantage and make time and money savings in the field of research and development (R&D). The tools used are distributed by hackers, enabling their application by any suitably motivated unit or criminal group with sufficiently high level of computer skills and knowledge. However, the review of the most important APT activities inevitably leads to the conclusion that in all of the aforementioned cases with the involvement (direct or indirect) of military component, they had the nature of actions targeting defense systems of a state, influencing the balance of traditional potentials and aiming to change the existing *status quo*. Therefore, no longer is APT limited to commercial purposes, but is still an important tool in the global strategy pursued by major players internationally. In particular by the United States, the People's Republic of China and the Russian Federation, which are the main poles transforming the global power structure.

In the near future, this tendency will not only be maintained but also intensified toward the development of new vectors of attack and software tools for them. Regardless of whether the cybernetic arms race is underway or an open international conflict in the form of military and commercial surveillance is implemented as APT. All the more so since *Advanced Persistent* Threats are related to the existence of the so-called security gap and "there is no technical or legal solution that can eliminate this vulnerability" [M-Trends®… 2013, p. 1], just as "human and system vulnerabilities that allow access to the network can never be fully dissolved" [Detecting the Enemy…2012]. In the face of increasingly effective measures taken against APT, it is expected that new variants will emerge in the near future using little known or completely new vulnerabilities. These days, the *Internet of Things* has the greatest potential in this field, and future APTs will certainly use the emerging *wireless sensor network* (WSN). In 2015, KasperskyLabs predicted that the year 2016 would see the decline of APT and they would be replaced by "deeper and more destructive attacks that are heavier to detect and track down cyber criminals" [Osborne 2015]. Further technological (r)evolution towards the broad implementation of such solutions as quantum and biological computers or artificial intelligence (AI) will bring IT security issues to an unknown level, leaving *Advanced Persistent Threats* in the domain of historical cyber threats.

Acknowledgement

No acknowledgement and potential founding was reported by the authors.

Conflict of interests

The author declared no conflict of interests.

Author contributions

Author contributed to the interpretation of results and writing of the paper. Author read and approved the final manuscript.

Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Boguslaw Olszewski – The author declared that he has no ORCID ID's

References

2009 Report to Congress of the U.S.-China Economic and Security Review Commission. (2009). Washington: U.S. Government Printing Office, [online]. 1 November 2009. Available at: http://origin.www.uscc.gov/sites/default/files/annual_reports/2009-Report-to-Congress.pdf [Accessed: 13 October 2016].

2012 Data Breach Investigation Report. (2012), [online]. Verizon (Website). Available at: http://www.verizonenterprise.com/resources/reports/ rp_data-breach-investigations-report-2012-ebk_en_xg.pdf [Accessed: 13 October 2016].

Advanced Persistent Threats Awareness. (2013), [online]. Trend Micro (Website). Available at: http://www.isaca.org/Knowledge-Center/ Research/Documents/APT-Survey-Report_whp_Eng _ 0213.pdf [Accessed: 13 October 2016].

Advanced Persistent Threats: A Symantec Perspective. (2011), [online]. Symantec (Website). Available at: https://www.symantec.com/content/en/ us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf [Accessed: 13 October 2016].

Andress, J. and Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham: Syngress.

APT: The Best Defense Is a Full Spectrum Offense. (2014), [online]. Zscaler, San Jose (Website). Available at: https://www.zscaler.com/pdf/ whitepapers/zscaler-apt-the-best-defense-whitepaper.pdf [Accessed: 13 October 2016].

APT: Zaawansowane trwale zagrozenie. (n.d.), [online]. Abbreviation Finder (Website). Available at: http://www.abbreviationfinder.org/pl/acronyms/apt_advanced-persistent-threat.html [Accessed: 13 October 2016].

APT28: A Window Into Russia's Cyber Espionage Operations? (2014), [online]. FireEye (Website). Available at: https://www.fireeye.com/content/ dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf [Accessed: 13 October 2016].

APTs. New waves of advanced persistent threats are vastly improved and smarter than ever. (2015), [online]. Haymarket Media. Available at: https://www.sans.org/media/press/SC-Mag-APT-eBook.pdf [Accessed: 13 October 2016].

Barnes, J.E. (2008). *Pentagon computer networks attacked*, [online]. Post: 28 November 2008. Available at: http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28 [Accessed: 13 October 2016].

Bequerel, S. (2013). *Wszystko, co powinienes wiedziec o APT*, [online]. Post: 22 November 2013. Available at: https://plblog.kaspersky.com/wszystko-co-powinienes-wiedziec-o-apt/696/ [Accessed: 13 October 2016].

Carvey, H. (2006). *More Real Threat Reporting*, [online]. Post: 18 August 2006. Available at: http://taosecurity.blogspot.com/2006/08/more-real-threat-reporting.html [Accessed: 13 October 2016].

Chen, P., Desmet, L. and Huygens, C. (n.d.). *A study on Advanced Persistent Threats*, [online]. Available at: https://lirias.kuleuven.be/ bitstream/123456789/461050/1/2014-apt-study.pdf [Accessed: 13 October 2016].

Clayton, M. (2010). *US oil industry hit by cyberattacks: Was China involved?*, [online]. The Christian Science Monitor (Website). Available at: http://www.csmonitor.com/USA/ 2010/0125/US-oil-industry-hit-by-cyberattacks-Was-China-involved [Accessed: 13 October 2016].

Cloppert, M. (2011). *Why Stuxnet Isn't APT*, [online]. Post: 24 March 2011. Available at: https://digital-forensics.sans.org/blog/2011/03/24/digital-forensics-stuxnet-apt [Accessed: 13 October 2016].

Cyber Definitions. (n.d.), [online]. NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia (Website). Available at: https://ccdcoe.org/cyber-definitions.html [Accessed: 13 October 2016].

Cyber Espionage. The Harsh Reality of Advanced Security Threats. (2011), [online]. Deloitte. Available at: https://www.isaca.org/ chapters1/phoenix/events/Documents/cyber_espionage.pdf [Accessed: 13 October 2016].

Detecting the Enemy Inside the Network. How Tough is to Deal with APTs? (2012), [online]. Trend Micro. Available at: http://www.trendmicro.co.uk/media/wp/apt-primer-whitepaper.pdf [Accessed: 13 October 2016].

Farber, D. (2013). *NSA reportedly planted spyware on electronics equipment*, [online]. Post: 29 December 2013. Available at: https://www.cnet.com/news/nsa-reportedly-planted-spyware-on-electronics-equipment/ [Accessed: 13 October 2016].

Gajewski, M. (2013). *Cyberataki typu APT nowym frontem wojny*, [online]. Post: 21 March 2013. Available at: http://www.chip.pl/news/bezpieczenstwo/luki-bezpieczenstwa/2013/03/cyberataki-typu-apt-nowym-frontem-wojny [Accessed: 13 October 2016].

Ghafir, I. and Prenosil, V. (2014). *Advanced Persistent Threat Attack Detection: An Overview*. Proc. of the Intl. Conf. on Advances In Computing, Electronics and Electrical Technology – CEET 2014. Institute of Research Engineers and Doctors, Kuala Lumpur, Seek Digital Library, pp. 154-158. DOI: 10.15224/978-1-63248-005-7-55.

Gostev, A. (2014). *Agent.btz: a Source of Inspiration?*, [online]. Post: 12 March 2014. Available at: https://securelist.com/blog/virus-watch/58551/agent-btz-a-source-of-inspiration/ [Accessed: 13 October 2016].

Greenert, J. and Welsh, M. (2013). *Breaking the Kill Chain. How to keep America in the game when our enemies are trying to shut us out*, [online]. Available at: http://foreign policy.com/2013/05/17/breaking-the-kill-chain/ [Accessed: 13 October 2016].

Harrel, Y. (2015). *Rosyjska cyberstrategia*. Warszawa: Wydawnictwo DiG.

Kissel, R. (ed.). (2013). *Glossary of Key Information Security Terms*. NISTIR 7298, Rev. 2, [online]. Gaithersburg: National Institute of Standards and Technology. Available at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [Accessed: 29 September 2018].

Kostecki, W. (2012). *Strach i potega. Bezpieczenstwo miedzynarodowe w XXI wieku*. Warszawa: Poltext.

Liang, Q. and Xiangsui, W. (1999). *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House.

Lord, N. (2018). *What is an Advanced Persistent Threat? APT Definition*, [online]. Mandiant. Post: 11 September 2018. Available at: https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition [Accessed: 13 October 2016].

Mandiant M-Trends. The Advanced Persistent Threat. (2010), [online]. Mandiant. Available at: http://static1.1.sqspcdn.com/ static/f/956646/23348947/1377032203613/M-Trends+by+Mandiant.pdf?token=rHV NRdmJOeNXpYxvBtLi1LiZcAk%3D [Accessed: 13 October 2016].

M-Trends® 2013: Attack the Security Gap. (2013), [online]. Available at: https://www2.fireeye.com/WEB-2013-MNDT-RPT-M-Trends-2013_LP.html [Accessed: 13 October 2016].

Osborne, C. (2015). *Security in 2016: The death of advanced persistent threats*, [online]. Post: 17 November 2015. Available at: http://www.zdnet.com/article/security-in-2016-the-death-of-advanced-persistent-threats/ [Accessed: 13 October 2016].

Passeri, P. (2012). *What is a Cyber Weapon?*, [online]. Hackmageddon (Website). Post: 22 April 2012. Available at: http://www.hackmageddon.com/2012/04/22/what-is-a-cyber-weapon/ [Accessed: 30 September 2018].

Rawnsley, A. (2011). *Fishy Chips: Spies Want to Hack-Proof Circuits*, [online]. Post: 24 June 2011. Available at: https://www.wired.com/2011/06/chips-oy-spies-want-to-hack-proof-circuits/#more-49990 [Accessed: 13 October 2016].

Skorobogatov, S.P. (2005). *Semi-invasive attacks – A new approach to hardware security analysis*, [online]. Cambridge 2005: University of Cambridge Computer Laboratory. Available at: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf [Accessed: 29 September 2018].

Smith, B. (2013). *Protecting customer data from government snooping*, [online]. Available at: https://blogs.microsoft.com/blog/2013/12/04/ protecting-customer-data-from-government-snooping/#sm.000q1t0tbw42e8x116s27 dp570ftt [Accessed: 13 October 2016].

Stoll, C. (1989). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday.

Tankard, C. (2011). Advanced Persistent threats and how to monitor and deter them. *Network Security*, no. 8, pp. 16-19. Available at: http://www.sciencedirect.com/science/article/pii/S1353485811700861 [Accessed: 29 September 2018].

Tracking GhostNet: Investigating a Cyber Espionage Network. (2009), [online]. Information Warfare Monitor, 29 March 2009. Available at: http://www.nartv.org/mirror/ghostnet.pdf [Accessed: 13 October 2016].

Trend Micro Deep Discovery. Ochrona nastepnej generacji przed atakami skierowanymi i APT, (n.d.), [online]. Available at: http://www.clico.pl/rozwiazania/producenci/trend-micro/trend-micro-deep-discovery [Accessed: 13 October 2016].

Virvilis, N., Gritzalis, D. and Apostolopoulos, T. (2013). *Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?* Proceeding UIC-ATC '13 Proceedings of the 2013 IEEE 10th International Conference on Ubiquitous Intelligence & Computing and 2013 IEEE

10th International Conference on Autonomic & Trusted Computing (UIC/ATC), IEEE Xplore, Washington, pp. 396-403, DOI: 10.1109/UIC-ATC.2013.80.

Biographical notes

Boguslaw Olszewski – PhD, student at the Institute of International Studies at the Wroclaw University. The area of his research interest is related to the broadly understood context of cyber warfare and cyber security. Participant of several conferences devoted to the aforementioned issues, author of articles and chapters in monographs. Participant in the NCN project on ethnic policy (UMCS in Lublin, 2013-2015). Leader and executor of internal research projects: *Evolution of the law of armed conflicts and international security* (2014, visit to Estonia), *International law aspects of cyber space militarization* (2014, visit to Amsterdam) and *Technopolies in the process of regionalization of cyber security* (Amsterdam 2015). In 2015 he held a three-month internship at the Faculty of Law at the University of Amsterdam and in April 2016 a two-week academic internship in Lithuania.

How to cite this paper

Olszewski, B. (2018). Advanced persistent threats as a manifestation of states' military activity in cyber space. *Scientific Journal of the Military University of Land Forces*, vol. 50, no. 3(189), pp. 57-71, http://dx.doi.org/10.5604/01.3001.0012.6227