TURKEY UNDER CYBER FIRE

The theater of cyberwar is changing and evolving by the minute. New threats, new attacks, and new actors are emerging daily, with Turkey likely being both the target and the attacker in many cyber attacks. Its young population, the nation's increasing use of technology, and growing nationalist ideas could place Turkish hackers as one of the main actors in the global cyberwar. However, a number of factors could doom Turkey to only have several different cyber militias rather than a well organized cyber army. Attacks targeting Turkey and the region could speed up the organization of such cyber attack capabilities.

Alper Başaran*

TURKISH POLICY QUARTERLY
Spring 2017

* Alper Başaran is the Founder of *Garnizon Bilgi Guvenligi*, a company specialized in penetration testing and cybersecurity consulting services working with government agencies and enterprises in Turkey.

Cyber attacks have become part of our daily lives. The last great offensive occurred on 12 May 2017 in a global attack that compromised over a quarter million computers worldwide. A ransomware (a malicious software that encrypts files on the computer it infects and asks for money to decrypt them) caused delays on German railways, almost halted the UK's National Health Services, and stopped production in some major French factories. This scenario unfolded on a global scale within a few hours.[1]

This ransomware was built using an exploit developed by the National Security Agency (NSA) and was leaked by Wikileaks, both of which are key actors in the current arena of cyber warfare. In March of this year, a group of hackers calling themselves "Shadow Brokers" released several hacking tools they claimed were stolen from a hacked NSA server. Among these was a powerful code attack exploiting a widely used Windows service. Within two months following the initial leak, one of the largest cyber attacks was launched, infecting hundreds of thousands of computers worldwide.[2]

This event perfectly illustrates the asymmetric nature of cyberwar; anyone with a certain level of computer skills can launch a global offensive. The grand cyberwar theatre involves not only countries, but also individuals and groups with political agendas.

Turkey has experienced an electronic transformation in the last 10 years, both in private corporations and government agencies. Turkey is also an important consumer of technology; it ranks 18th on the list of countries with the highest number of internet users,[3] and fourth with the most Facebook users.[4] These two factors have shaped the business and economic scene in the country for the last decade, making it increasingly reliant on technology. Turkey has then become an interesting target for criminals who abuse technology and target other countries for intelligence purposes.

Turkey took its first step related to cyber security at the government level in 2012, followed by the creation of the Turkish Computer Emergency Response Team (CERT), the Turkish Army Cyber Command, and the inclusion of cyber security related issues in national security documents.

[1] Andrew Liptak, "The WannaCry ransomware attack has spread to 150 countries," *The Verge*, 14 May 2017, https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries

[2] "WannaCry related interim timeline," *Security and Risk*, http://securityandrisk.blogspot.com.tr/2017/05/let-me-share-timeline-i-constructed.html

[3] "Top 20 Countries in Internet Users vs. All the World," *Internet World Stats*, 31 March 2017, http://www.internetworldstats.com/top20.htm

[4] "Leading countries based on number of Facebook users as of April 2017 (in millions)," *The Statistics Portal*, https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/

"Turkey ranks 18th on the list of countries with the highest number of Internet users, and fourth with the most Facebook users."

In the last decade, Turkey was the target of several major cyber attacks; some were openly disclosed as such, and others left in the dark due to either poor post-attack analysis or to executive decisions. One of the cyber attacks with some level of proof is the explosion that happened on the Baku-Tbilisi-Ceyhan (BTC) pipeline in 2008. Several aspects of the incident show this was likely the result of a cyber attack. For one thing, operators that were continuously monitoring the pipeline with state-of-the-art equipment, noticed the explosion some 40 minutes after it occurred. This is interesting because the monitoring systems should have alerted the operator even in the case of a slightest pressure difference, let alone a full-scale explosion at one of the relay stations. Further investigation conducted by committees, including experts from participating countries, have revealed other suspicious activities that would hint to a cyber operation, such as the CCTV system being hacked and around 60 hours of security camera footage getting erased. Sources speaking to Bloomberg on the subject mentioned "a single infrared camera not connected to the same network captured images of two men with laptop computers walking near the pipeline days before the explosion, according to someone who reviewed the video. The men wore black military-style uniforms without insignias, similar to the garb worn by special forces troops." If this was really a cyber attack conducted by Russia, it would certainly fit their political agenda as it could support the strong message against the BTC pipeline, together with the kinetic offensive against Georgia.[5]

"Kinetic war" is a term used for the regular way of conducting war with boots on the ground and air force support. Cyberwar, on the other hand, requires much less resources and any direct involvement can easily be denied by the government.

Cyber Security Actors in Turkey

Before any military cyber force, Turkey had several "cyber militias." To put this into context, most Turkish nationals have strong nationalist feelings and young computer hackers are easily motivated by the idea of supporting their country. Hacker groups such as "Cyber Warrior" or "Ayyildiz Tim" have been conducting "cyber operations" since the beginning of the 2000s. These hacker groups usually use ranks similar to the ones in the army. They conduct campaigns which target countries that

[5] Dan Goodin, "Hack said to cause fiery pipeline blast could rewrite history of cyberwar," *Ars Technica*, 11 December 2014, https://arstechnica.com/security/2014/12/hack-said-to-cause-fiery-pipeline-blast-could-rewrite-history-of-cyberwar/

"In 2012, a denial of service attack targeted Turkish Airlines, which resulted in an estimated loss of around 250,000 dollars."

Turkey might have tense political relations with, historically or *pro tempore*. While these operations rarely hint at advanced cyber operation skills – which would be required to conduct the above mentioned pipeline attack – they provide inspiration for teenagers who are eager to become hackers. These groups have recruiting schemes and frequently use arguments that would appeal to nationalist feelings, resulting in the belief of serving the greater interest of the country among the recruits. Targets of the operations are usually civilian systems, such as the website of small and medium corporations or social media accounts.

The extent to which these "cyber militias" are employed, used, or managed by any branch of the government is difficult to measure. Members of these groups often claim that they passed information they gathered from hacked servers to government officials. The fact that these groups mostly operate in a way that leaves the victim compromised, such as defacing the victim's website with logos and other political messages, would make these operations rather useless as far as intelligence is concerned. NSA leaks show us the extent of the effort put to remain undetected after having infiltrated a computer system and gathered intelligence for a long period of time. Thus, it is very unlikely that defacing the website of a victim and letting them know that they are compromised would have any practical use. Russia and China are other countries that have access to nationalist or patriotic hackers and are suspected to employ them. Russian Duma Deputy Nikolai Kuryanovich once described the hackers as Russia's "information soldiers."[6]

"Cyber militias" are a result of the asymmetric nature of cyberwar akin to guerilla warfare. Another type of actor are the hacktivist groups, and are usually politically motivated. Turkey had to deal with such a group in the past. Calling themselves "Redhack," the Marxist-Leninist group conducted a series of high profiled attacks against government agencies. The group was disclosing confidential information such as the identities of police informants and defacing government websites for propaganda purposes, however a series of arrests made in the last couple of years to curb the activities of this group was effective and thus there have been no recently reported attacks related to this group.[7]

[6] Derek S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power* (Washington DC: Georgetown University Press, 2012), p. 184, http://bit.ly/2pNRsNO

[7] "Groups hack MİT, TFF, police department's website," *World Bulletin*, 19 July 2012, http://www.worldbulletin.net/?aType=haber&ArticleID=92699;

Most Recent Cyber Attacks in Turkey and its Region

Cyber attacks can have a variety of goals including propaganda, intelligence gathering, and the denial of service. While patriotic hackers initiate attacks to have a psychological impact, these groups also conduct denial of service attacks. These attacks aim to stop any internet facing system by using all of the available resource of the target system. For example, a denial of service attack targeted Turkish Airlines, the national flag carrier, in 2012.

The six-hour attack resulted in an estimated loss of around 250,000 dollars and thousands of customers that could not purchase tickets or proceed with online check-in. Actors behind Distributed Denial of Service (DDoS) attacks are almost impossible to detect due to the technical nature of these attacks. Connection requests from anywhere and even spoofed sources overwhelm servers, making it impossible for servers to accept the connections of legitimate users. The impact of large scale DDoS attacks was already well established when Estonia was hit in 2007 following a disagreement with Russia on the location of a World War II statue. Attacks were planned and advertised in Russian and pro-Russian chatrooms and forums, and some even had a step by step manual on how to take part in the attack and a list of potential targets. DDoS attacks can be launched by any hacktivist group with a political agenda and all they need are computer skills.

"It is important to build cyber warfare capacities, rather than conduct a military operation, as it is cheaper and allows any country to deny involvement."

Computer resources can be lent by patriotic computer users, such as was the case in Estonia, or anyone supporting a common cause, such as the attacks conducted by the group Anonymous. Anonymous was using a free software that anyone could download to their computer to take part in the "operation." Turkey witnessed the largest DDoS attack in its history in December 2015, which was organized by Anonymous.[8] This attack targeted the Turkish domain name infrastructure and disrupted almost all websites and internet services in the country.[9] The hacktivist group Anonymous

[8] "Turkish banks & government sites under 'intense' attacks on Christmas holidays," *RT*, 26 December 2015, https://www.rt.com/news/327119-turkey-banks-cyber-attacks/

[9] The "domain name infrastructure" allows computers to locate a website address. When any user enters an address in their browser it is converted to an IP address, which is the way computers talk to each other on the Internet (which would be for TPQ). Computers cannot find the website they have to connect to if the infrastructure responsible to revolve the website address as we know it to the IP address fails.

claimed responsibility, however the *modus operandi* of the attack and the fact that it occurred at a time when Turkish-Russian relations were tense, to say the least, might be the main clue hinting to Russian involvement. Just one month prior to the DDoS attack, a Russian Sukhoi SU-24 aircraft was shot down by a Turkish F-16 triggering a full scale diplomatic crisis.

Denial of Service attacks are widely advertised as a service in criminal hacking forums and the deep web. Prices depending on the duration and the intensity of the attack range from 50 dollars for a small attack, and up to 700,000 dollars for a full day attack that could easily cripple a whole city's internet connection.[10] DDoS attacks are also often the by-product of a different kind of attack; malicious software – also known as malware – which infects computers and can have several different tasks. For example, Ransomware, as mentioned earlier, encrypts files and asks for a ransom. Trojans, another example of malicious software, allows the attacker to remotely control the victim's computer. Other types of malware turn the infected computer into a "zombie" by turning it into a member of a Botnet (Robot Network), essentially allowing the attacker to use the infected computer in DDoS attacks. In this case, home computers and ADSL routers become "attackers" and send connection requests to the target chosen by the attacker. Botnets are a growing problem, especially given the increasing importance of Internet of Things;[11] we increasingly witness attacks that use our own connected devices as "zombies," such as security cameras connected to the internet.[12] On a global scale, malware is the main cause of Botnets and research conducted by antivirus companies show that Turkey is one of the most infected countries; over 40 percent of computers in Turkey are infected by malware according to one study in particular. It is difficult to obtain real data on the subject, however it seems that Turkey has been both the target and the attacker in many DDoS attacks.[13]

Turkey has been subject to attacks by more sophisticated actors as well, as cyber operations from Iran, Lebanon, and other important players in the Middle East have been detected. Attacks such as these require a higher level of technical capacity than a regular criminal hacker, hacktivist, or patriotic hacker. Also known as Advanced Persistent Threats (APT), attacks such as these are the most dangerous as they are difficult to detect, and their persistent nature ensures high success rates. APT attacks

[10] Pierluigi Paganini, "How much costs a DDoS attack service? Which factors influence the final price?" *Security Affairs*, 26 March 2017, http://securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html

[11] The Internet of Things (IoT) refers to a network of devices capable of collecting and/or exchanging data. Any smart appliance that can be connected to the Internet wirelessly or with a cable can be considered an IoT device.

[12] Lucian Constantin, "Thousands of hacked CCTV devices used in DDoS attacks," *PC World*, 28 June 2016, http://www.pcworld.com/article/3089346/security/thousands-of-hacked-cctv-devices-used-in-ddos-attacks.html

[13] "Countries with the highest rate of malware infected computers as of 4th quarter 2016," *The Statistics Portal*, https://www.statista.com/statistics/266169/highest-malware-infection-rate-countries/

are usually conducted by sovereign nations as they require important financial and technical resources, yet are less risky than military operations. One of the best examples for these attacks is STUXNET, discovered in 2010, which is a malware especially designed and developed to target nuclear reactors in Iran to hinder the Iranian nuclear program.[14] Operation Orchard of 2007 saw the Israeli Airforce bomb an alleged nuclear reactor in Syria.[15] This operation involved huge risks both before and during the attack, as Israeli aircrafts faced the danger of being shot down which would undeniably reveal Israel's involvement in the operation. STUXNET, on the other hand, is a small piece of software and, although allegedly developed by the NSA, no direct proof about its origin has been found. This shows the importance of building cyber warfare capacities rather than conducting a military operation, as it is cheaper and allows any country to deny involvement.

"The period following the failed coup has seen a growing demand for national cyber security solutions in order to replace imported ones."

Conclusion

Placed in a difficult geopolitical area, Turkey is constantly under attack. The failed coup attempt on July 15th 2016, demonstrated how quickly and dangerously the political situation can change. The period following the failed coup has seen a growing demand for national cyber security solutions in order to replace imported ones. Nevertheless, not all cyber attacks are as sophisticated as STUXNET. Both government and private websites are constantly under attack and defacements are used as a means of propaganda by the hacking individuals or groups. The numbers are impressive: 484 Turkish government websites are shown defaced on one of the repositories where hackers brag about their accomplishments, and the number increases daily. It is common for websites to be used to publish propaganda messages for various terrorist organizations.[16] These small operations are usually conducted by individuals or small groups, and although they seem to be motivated politically, more often than not these attacks serve as a way for newcomers to earn respect in the criminal hacking community. In response, in 2014 it became obligatory for governmental agencies and companies operating in critical sectors

[14] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, 3 November 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[15] Erich Follath and Holger Stark, "How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Spiegel Online*, 2 November 2009, http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html

[16] *Zone-H Unrestricted Information*, http://www.zone-h.org

such as energy, aviation, or the government sector to form their own Computer Emergency Response Team (CERT) to mitigate such attacks and coordinate with the national CERT.[17] So far, however, the majority of CERTs cannot operate effectively due to a lack of human resources and technical training.

Spy agencies such as the NSA and the British Government Communications Headquarters have demonstrated their ability to use hacking as an important source of intelligence gathering, while Russia seems to use cyber warfare activities for kinetic operations. With the increasing penetration of technology in military systems, a compromise could hinder the military capacity of any country. The Turkish Cyber Command, for example, focuses on the prevention, detection, and mitigation of attacks that would target military systems. On the other hand, the civilian Turkish National Cyber Security Incident Response Team (TR CERT) provides support to corporations and government agencies. This model shows a cyber warfare capacity that mostly focus on the defensive side, aiming to prevent any infiltration or large scale attack that would target Turkey. While unofficial sources mention certain offensive capabilities, confirming the existence of such projects would be impossible. Turkey regularly takes part in cyber defense exercises such as "Locked Shields," organized by NATO, which aims to increase the cooperation capabilities and information sharing among its members. These exercises increase the ability of participating countries to counter a possible cyber attack and reach a higher level of cooperation during the attack.[18]

In the last six months, the Turkish Information and Communication Technologies Authority (ICTA) has given open support to projects that would help recruit people with more "offensive capabilities" or, hackers. One such initiative was the "Cyber Star" hacking challenge, for which over 25,000 people registered and winners would be offered contracts in government agencies, according to ICTA. This shows that Turkey is trying to develop a more proactive approach to cyber security, of which there is evidently a growing need.

[17] T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü, "Kurumsal Some Kurulum ve Yönetim Rehberi," [Guide For Creating and Managing National Cyber Incident Response Team], 4 October 2016, http://www.udhb.gov.tr/doc/siberg/Kurumsal_SOME_Reh_V1.pdf

[18] "Locked Shields 2017," *CCDCOE*, https://ccdcoe.org/locked-shields-2017.html