PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

STRATEGIC FILE

No. 4 (40), February 2014 © PISM

Cyberterrorism: The Threat That Never Was

Andrzej Kozłowski, Kacper Rękawek, Marcin Terlikowski

If the seriousness of a given "emerging security threat" is measured by the number of recent analyses devoted to it or the proliferation of experts studying it, then cyberthreats must now surpass the dangers of offline terrorism and energy security. While all issues "cyber" attract a high level of policymaker attention, another threat seems to have been forgotten and marginalised: cyberterrorism. To an extent, the evolution of cyberterrorism mirrors that of "regular" terrorism, which erupted as the "weapon of the weak," and after a state-sponsored phase seems to be returning to its sub-state or even "lone wolf" roots. Cyberthreats, on the other hand, originally of a sub-state nature, are now mostly in the domain of state entities that have not yet made the decision to launch state-sponsored cyberterrorism.

In recent years, cyberattacks have become one of the most broadly discussed challenges to the security of the modern state. With the rising tide of malicious actions in cyberspace, followed by billion-dollar losses and damages to the credibility of the targeted entities, governments began to establish strategies, policies, agencies and procedures to defend against cyberthreats. Nevertheless, the perpetrators of cyberattacks are arguably still way ahead of the defensive measures taken by both governments and private businesses. Chilling news about large data thefts, online fraud, or even damage to physical devices caused by malicious software, such as Stuxnet's alleged effects on the Iranian nuclear programme demonstrated, compound fears of the apparently limitless ability of cyberattacks to cause harm. In this context, the debate about the once vividly discussed, then largely forgotten threat of cyberterrorism is re-surfacing. At its core is the question of whether the world will soon witness a major terrorist attack in which the carrier of deadly force is a virtual piece of software rather than a suicide bomber.

The Dark Force Beneath

According to statistics provided by companies that operate on the ICT security market, the evolution of the cyberthreat landscape has been particularly dynamic over the last two years. By the end of September 2013, the number of unique pieces of malware (i.e., software designed to perform cyberattacks, such as stealing data or paralyzing computers) grew to more than 170 million.[1] With each single instance of malware typically responsible for hundreds of thousands of attacks or attempts thereof, the scale of malicious activity on the internet is huge. In 2012, around 250,000 attempted attacks were being stopped daily on websites alone.[2] Another good indicator of the scale of online security breaches is spam in the form of unrequested advertisements sent via e-mail, social networking sites, chats or other channels of internet-based communication, typically promoting gray-market drugs or sexual/dating portals, and less frequently but significant nonetheless, fake financial services. In September 2013 alone, the volume of spam

[1] *McAfee Labs Threat Report: Third Quarter 2013 Executive Summary*, www.mcafee.com.

[2] "Internet Security Threat Report 2012," *2012 Trends*, vol. 18, April 2013, www.symantec.com.

was estimated to be just shy of four trillion messages, a sharp increase compared to beginning of 2013, when just over a trillion messages were being distributed monthly, even then flooding the e-mail boxes of virtually every Internet user in the world.[3]

These data reveal some key trends. The growth in the sheer volume of cyberattacks testifies to the argument that the number of actors who engage in damaging actions in cyberspace is increasing. New individuals and groups enter the dark nets of cyberspace, where information about vulnerabilities that provide access to otherwise protected systems in popular software are traded, the electronic tools to break into safeguarded systems are built and sold (scripts, trojans, worms), and illegal networks are created and leased out to allow large-scale attacks (so called botnets). This "Dark Internet" ("darknet") or "Deep Web," as it is often referred to, is now a thriving part of cyberspace, even if it remains largely invisible to the average network user, at least until they become the targets of an attack.

Target Acquired: States

A distinctive category of cyberthreats are so called targeted attacks, which are aimed at stealing sensitive data from a selected group of internet users, or even a precisely defined single user (e.g., a global corporation or a government agency). In 2012, the number of such carefully crafted attacks grew by 42% and new techniques were employed to get the data targeted.[4] The best known of these attacks was the Stuxnet worm, discovered in 2010. It was allegedly used to paralyze certain industrial systems, was proliferated in the Middle East, and was dubbed the very first "cyberweapon", as it was suggested that its target was Iranian nuclear facilities.[5] Even more public attention came with cyberattack campaigns against government agencies and industrial leaders in the U.S. and EU, revealed in late 2012. A variety of specialised tools was used to get access to sensitive information stored in systems run by more than 100 distinct entities (defence companies and other manufacturing industries). In total, thousands of terabytes of data were stolen over a period of a few years by unknown perpetrators (it is thought the origin of the attack was China, allegedly from one of the Chinese People's Liberation Army's military units).[6]

This is a telling trend, as it points to the fact that the aim of the attack is no longer only to make money from online fraud or spam targeted at a huge number of average users. The typical victims of this new kind of attack are carefully chosen government agencies and leading industrial companies, rather than random individuals. In other words, for these types of targeted attacks, the driving logic behind the malicious activity is reversed: it is not the number of victims that ensures success (e.g., when a 0.01% out of a million targeted users provide an attacker with login details for an online bank account), but rather the depth and complexity of the attack pointed at a very narrow group of targets that brings results. This may suggest that the true goal of the attacks is a desire to acquire sensitive—and most probably specific—information. Thus, the question of who is behind those attacks can be answered only by deducing "who benefits." Since these operations are driven by the demand for specific data, most likely it is the adversaries of the targeted states or corporations—other governments or competitors—that are behind these kinds of attacks. When the attackers gain access to confidential information, they might aim, for example, to formulate market strategies that exploit their competitors' weaknesses, better prepare for negotiations, or simply learn more about particularly cutting-edge technologies. The Stuxnet and Flame worms suggest one more potential use for such attacks—to actually disturb the *physical* operations of selected industries to meet specific goals in the context of ongoing political conflict.

To classify these kind of attacks as "normal" industrial espionage, or even cyberespionage would be to misunderstand them. In fact, they are evidence that cyberspace, once dominated by skilled individuals, is increasingly falling under state control, often for the benefit of these states' own enterprises or large national corporations, and it is a worrying trend. For years it had been individual hackers or groups of criminals who were responsible for virtually all cases of cybersecurity breaches. Cyberspace itself was portrayed as an area in which weak actors may challenge states. It was an attractive force multiplier for various non-state entities, either motivated by money (cybercriminals), policy (so called hactivists,

---

[3] *McAfee Labs Threat Report*, *op. cit.*

[4] "Internet Security Threat Report 2012," *op. cit.*

[5] See, e.g., R. Lagner, "Stuxnet Secret Twin," *Foreign Policy*, 19 November 2013, www.foreignpolicy.com.

[6] "Exposing One of China's Cyber Espionage Units," *Mandiant APT1*, www.mandiant.com.

responsible for defacing website or creating other forms of online protests) or psychology (individual hackers, such as the hacker icon Kevin Mitnick).[7] This picture is now undergoing a deep change. States have recognised the potential of hackers and have arguably employed them in pursuit of the government's national policy and economic goals. How this has been achieved (most likely through dedicated cyberespionage agencies or military units, or possibly through criminal groups of hackers hired for specific attacks) is of secondary importance, since the crucial issue is that malicious activity in cyberspace will now start to follow state, rather than non-state logic. This will have a deep effect on the motivations for attacks, the selection of the targets and means of attacking them. One consequence of this is that the notion of state security in cyberspace, even if only born recently, already needs to be updated.

A Short History of International Terrorism

To date, whenever the security of the state in cyberspace was discussed, the most serious threat indicated by experts was cyberterrorism. Defined as the malicious use of the internet or other ICT networks to cause physical damage or even casualties, this concept was born in the 1990s, when the most-developed states discovered that they were prone to manipulations of their ICT systems, which could be taken down or disturbed even by single individuals. A scenario of a "cyber-Pearl Harbor" was created in which a series of cyberattacks would lead to power blackouts, accidents at industrial facilities or utility distribution networks (oil, gas, water, sewer) or cause transportation catastrophes, all of which could include physical damage, environmental contamination, and even human fatalities.[8] As mass media rather robustly picked up on this concept, the possibility of a terrorist cyberattack on what then became known as "critical infrastructure," became the most discussed cyberthreat. The menace of a lone terrorist taking down the whole country with just his laptop suddenly became a major security threat, one for which the states began to seriously prepare (particularly following the discovery of just such a laptop containing specialised software used in U.S. utility control rooms and power plants in a cave in Afghanistan that had sheltered Al Qaeda members). Cyberterrorism began to be portrayed as the "terrorism of the future." After the 9/11 attacks, it was seen as a key security challenge to a world dependent on such networks.[9]

There are some striking similarities between the evolution of the perception of cyberthreats and the history of "classical" terrorism, particularly in terms of the development of the relationship of individuals to states. The modern phenomenon of terrorism emerged in the second half of the 19th century with the pan-European wave of anarchist violence directed at civilians and government officials alike by mostly individual actors who acted independently of any state encouragement or control.[10] It was only after World War I and the onset of the anti-colonial or nationalist wave of terrorism that various states made their first attempts to actively engage with terrorist groups and organisations. The motto of "the enemy of my enemy is my friend" fuelled this trend in the interwar period. Croat Ustaše, keen on abolishing Yugoslavia and establishing an independent Croatia, found receptive, anti-Yugoslav political audiences in Bulgaria, Hungary and Italy. Consequently, after World War II, the Algerian National Liberation Front (FLN), which was combating the French in Algeria between 1954–1962, was supported by various Arab states, most notably Nasser's Egypt, and between 1955 and 1959 the National Organisation of Cypriot Fighters (EOKA) fought the British with Greece's backing. Thus, state-supported terrorism was born. But it was to reach its zenith during the next two phases in the history of terrorism: the so called New-Left (which combined both leftist and nationalist-separatist terror), then the religious wave.

Between the late 1960s and late 1980s, terrorist outfits received support from various states that enabled these groups to prolong and advance their operational capabilities. For example, the Popular Front for the Liberation of Palestine was armed by the Soviet Union (1970s), and the Irish Republican Army obtained arms and funding from Col. Qaddafi's Libya (1980s). Moreover, not only did some states support certain terrorists but some went further and, to an extent, completely took over the decision-making processes in the terrorist organisations. The German Democratic Republic's animating and sustaining of the Red Army

---

[7] See, e.g., "Networks and Netwars: The Future of Terror, Crime, and Militancy," J. Arquilla, D. Ronfeldt (eds.), *RAND Report*, 2001.

[8] See, e.g., E. Gatzke, "The Myth of Cyberwar," *International Security*, vol. 38, iss. 2, 2013, pp. 41–73.

[9] See, e.g., A. Rathmell, "Cyber-terrorism: The Threat of the Future?," *RUSI Journal*, vol. 142, no. 5, October 1997, pp. 40–45, reprinted by RAND in 2003.

[10] See, D.C. Rapoport, "The Four Waves of Modern Terrorism," www.international.ucla.edu/cms/files/Rapoport-Four-Waves-of-Modern-Terrorism.pdf.

Faction throughout the 1970s and the 1980s is one of the most prominent examples of this. Some countries not only provided resources but also effectively founded a terrorist entity, such was the case in the early 1980s with the Iranian Revolutionary Guards Corps, a branch of the post-revolutionary Iranian military, and the Lebanese Hezbollah. Other states provided terrorist groups with shelter and wittingly or unwittingly assisted their international activities, such as the case with Sudan and the Islamic Emirate of Afghanistan creating safe havens for Al Qaeda throughout the 1990s. The beginning of the 21st century saw the U.S.-led "global war on terror" (GWOT) which targeted both terrorist actors and some of their real or imaginary state sponsors, such as Saddam Hussein's Iraq.

Nonetheless, the elevation of Al Qaeda to the level of a global threat seemed to herald the return of non-state actors as the main "providers" and perpetrators of terrorism. GWOT appeared to be a major vindication of "netwar" theory—a form of low-intensity conflict waged by networked entities such as small and dispersed terrorist cells or larger internationalised insurgent-terrorist organisations. Among these were the likes of the Somali Al-Shabaab, a jihadist beneficiary of the post-1991 state failure in Somalia and a leading actor in the Somali civil war, and the Iraqi-Syrian Al-Nusra Front, initially a Syrian offshoot of Al Qaeda's Islamic State of Iraq, which has morphed into one of the most-discussed rebel factions in the Syrian civil war, attracting individual "foreign fighters" from around the world. What is more, fear and attacks perpetrated by so called lone wolves (e.g., the terrorist conspiracies of Anders Breivik) appear to have only strengthened the global conviction of the return of the non-state actor to the forefront of terrorism. Thus, one could claim that terrorism in the 21st century has returned to its non-state roots, and in the post-GWOT age will most probably be perpetrated by a variety of individual actors empowered by globalisation and remaining beyond the control of state apparatuses. If we were to accept such a theory, then the question must be posed and answered about how all of this relates to cyberthreats, or precisely cyberterrorism, as the alleged terrorism of the digital age.

Terrorism in Cyberspace?

At first glance, the development of the threats in cyberspace seems to mirror the evolution of "classical" terrorism. In the 1990s, when the internet went global and the number of users began to grow exponentially, cyberattacks were perpetuated and malware was created by individual hackers, much like individual terror acts that marked the birth of this phenomenon in the early 20th century. However, the difference lays in the political motivation of the attacks, or rather lack thereof. Early hackers tried to demonstrate their skills or to play a joke, rather than pursue any particular ideology or policy option through their activities. Many examples of such arguably clueless actions, in which manipulations in cyberspace led, or might have led, to physical damage, could be invoked.

In 1997, a hacker was able to disrupt the main telecommunications line at a small airport in Worcester (Massachusetts, USA) for six hours. The control tower could not contact planes, which posed a direct threat to the life of their passengers. However, the hacker was alleged to have done it to demonstrate his computer skills but did not intend to hurt anybody.[11] In 2000, an Australian hacker manipulated a waste management system and released millions of litres of sewage to rivers and creeks. What followed was a serious contamination of the environment.[12] Again, it was a case of a cyberattack that resulted in actual physical damage but was not politically motivated. The individual wanted to take revenge on the local government council, which had rejected his job application.

At the beginning of the 21st century, cyberattacks slowly became a tool of organised groups of hackers and were used to make money. Online fraud started to generate millions of dollars in income for professional cybercriminals, who thrived in an environment with largely unaware users who were incapable of protecting sensitive data such as logins or passwords. Consequently, the notion of cyberterrorism gradually disappeared from the debate on cybersecurity. But, fuelled by cybercriminals' desire to earn even more money, cyberattacks became more serious, sophisticated, well-planned and much harder to detect than ever before. Thus, the significant know-how and potential to perpetrate various kinds of cyberattacks was born.

---

[11] T. Szubrycht, "Cyberterroryzm jako nowa forma zagrożenia terrorystycznego," *Zeszyty Naukowe Akademii Marynarki Wojennej*, nr 1, 2005, p. 179.

[12] *Ibidem*.

In 2007, a sudden wave of cyberattacks on networks in Estonia demonstrated, as was later acknowledged, how the potential of cybercrime could be used in a political fight. The malware typically used to send spam from illegal computer networks called "botnets" was used this time to generate artificial internet traffic that overloaded Estonian servers and made all internet-based services temporarily unavailable across the country (a Denial-Of-Service attack). It would not have been possible to target an entire country if various organised cybercrime groups had not cooperated in some form with politically motivated actors.[13] From 2007 on, the steady increase in targeted cyberattacks and the profile of the victims seem to support the argument that there is more of a political motivation behind the attacks. When there is a large-scale attack on a government agency, there should be no doubt about other states' agents being behind it. If large companies are targeted and the retrieved data does not allow for quick access to money, the typical motivation behind such an attack, it may be useful from the perspective of rival corporate actors, especially those closely tied with their home state apparatus.

Consequently, an argument can be made that either the state had entered into a kind of practical alliance with non-state actors (cybercriminal groups), considering them proxies in cyberspace, or had established specialised cybercrime units, tasked with conducting cyberespionage campaigns targeted at both rival government agencies and businesses. As various sources indicate, the roots of some of these campaigns can be traced back to China or North Korea. While these countries deny any link to cyberespionage acts, it seems logical that governments that do not have an economic or military advantage over the U.S. or Western Europe, and at the same time can be considered political adversaries of America and its European allies, may seek sensitive information that would help them close this gap or simply widen their political options.

Risks of Cyberterrorism

This situation could be a cause for concern. Any state in conflict with the international community may consider using specially designed malware as a "weapon of the weak." It not only can provide anonymity, making it difficult for the victim to attribute responsibility for a given cyberattack and, consequently, retaliate (in any form), it also is relatively cheap to hire or train a hacker (or group) to conduct such an attack (definitely cheaper than developing a WMD programme, for example, which is broadly considered a guarantee of regime survival). From here, there is seemingly only one step to state-inspired and state-sponsored cybersabotage and cyberterrroism.

Despite forecasts about the forthcoming, unavoidable threat of cyberterrorism, so far there has not been a single cyberattack that could be classified as cyberterrorism, either state-assisted or aided or not. Thankfully, terrorist organisations have demonstrated a lack of expertise in this field as they have proved themselves unable to organise, conduct or sustain a prolonged, simultaneous cyberattack on multiple targets. For example, the electrical power grid seems to be and has been identified by security experts as a desirable target for a cyberterrorist attack. But, the networks consist of a range of redundant systems. The process of neutralising them would demand the use of a lot of sophisticated malware, highly specialised experts, as well as time and money to buy not only information about the vulnerabilities and relevant software (from the darknet) but also the required hardware. All of these seem to be outside of the reach of the current capacity of terrorist organisations.

Beginning with the human factor, it is notable that ICT experts hardly ever feature in terrorist ranks. In-house development or grooming of skilled hackers, after all, is a much harder task to accomplish than training and fielding suicide bombers, for example. Moreover, even the presence of ICT experts amongst the members of a given terrorist organisation or conspiracy, does not yet solve all of the issues related to cyberattacks. One would need much time to prepare a complex cyberattack, as effective malware cannot be created overnight to meet the goal of inflicting physical damage, not least because it takes time to actually identify the most valuable targets and assess their weaknesses. Further, it often goes unnoticed that such work would have to take place in a relatively secure location, one equipped with powerful computers and a reasonably fast internet connection. Some pieces of hardware are essential for any cyberattack, while

[13] M. Terlikowski, "Cyberattacks on Estonia: Implications for International and Polish Security," *The Polish Quarterly of International Affairs*, no. 3, 2007.

a more complex attack would surely demand more computing power and a really fast landline connection (e.g., fibre).

Apart from these technicalities, cyberattacks are hardly ever as spectacular as terrorists typically want. Thus, a successful cyberterrorist attack must be repeated, so that not only the authorities but also the general public become aware of the fact that a given target's breakdown (water, electricity, banking, social services, etc.) is not due to a one-time chance malfunction but the result of mischievous behaviour on behalf of a sub-state entity. In short, a terrorist entity would need to not only obtain cyberattack experts and basic capital but also most preferably multiply its attacks so that a given plot could be of a prolonged and serious nature.

Even if a terrorist organisation—state assisted or not—was to overcome these difficulties then it still needs to take into the account the fact that the effects of cyberattacks are gradual and materialise slowly. Even the most sophisticated malware to date, "Stuxnet," which temporarily disrupted Iran's nuclear facilities, did so only after months at work. This does not feature in terrorists' "action-reaction" mode of operations in which a sudden, although well-prepared, rehearsed and well-aimed strike, produces an immediate gross over-reaction on behalf of the security apparatus. The terrorists are probably fully aware of the fact that the world of *Live Free or Die Hard*, in which an individual hacker almost singlehandedly shuts down the government of the United States, is still a Hollywood fantasy which they are not capable of imitating. In addition to this, any attempt at imitation will most likely yield less tangible results than an outright series of bombings that would not only cause physical damage but successfully install fear into society. In short, the reality of 21st century terrorism has more to do with the original *Die Hard*, which depicts a hostage-taking situation by a group of criminals masquerading as politically motivated terrorists, and not its 2007 sequel.

Three New Threats

Nonetheless, the fact that cyberterrorism as such is not yet with us does not mean that terrorists shun IT technology. Their further utilisation of this technology is likely to result in the development of certain terrorist threats connected with cyberspace. The first one is a continuation of current methods of using the internet to communicate with new members, radicalise them, fundraise and exchange information about the scheme, how to construct bombs, or share other vital information. Terrorists are already doing it now, and in the future they will increasingly rely on internet communication to meet such goals. Thus, we might be witnessing an even more profound shift towards cyberspace on behalf of various non-state actors, which indeed are likely to consider it a force-multiplier. The only difference is that cyberspace activities will not have a "weapon" dimension and rather fall under the "support" sphere.

The second threat assumes close cooperation between terrorists and cybercriminals. This partnership may be that the latter are hired by the terrorists to steal money or gain valuable information about critical elements of infrastructure. This scenario looks probable, but it is necessary to consider the financial limits of most terrorist groups, which prefer to invest in classical methods such as training suicide bombers, rather than engage in cooperation with unreliable cybercriminal groups.

The third and most grave threat prediction foresees a cyberattack carried out simultaneously with a conventional attack. A suicide bomber could detonate a bomb in the city centre and, at the same time, cyberterrorists could strike against an emergency telephone line (such as 911 in the U.S.). Such an attack may play out as a force multiplier and strengthen the casualties and damage of the conventional action. Such a scenario, not yet likely however, is in tune with the Hollywood vision of the emerging security threats. This may be the most likely threat as a relatively small and easily conducted cyberattack may severely multiply the effects of a physical assault on a given target. The disruption of rescue communication channels seems to be particularly attractive for its unpredictable consequences on the evacuation and treatment of those injured in such a blast. Thankfully, the world and its terrorists, or their backers, seem not to be there yet.