CHAPTER

19

From Cyber Terrorism to State Actors' Covert Cyber Operations

Jan Kallberg, Bhavani Thuraisingham

INTRODUCTION

During the first 20 years of the Internet era there was a widespread fear of threats from the Internet, but in reality it was fairly secure. The limited abilities and resources of the early attackers contained the threat to criminal activity and marginal damage. Recent advancements in client computer security, in conjunction with the impact of time and Internet maturity, have created a population at ease and with and trusting of the Internet. In reality, the Internet has a reverse trajectory for its security, where the Internet has become more unsafe over time. The threat no longer engulfs just individuals and businesses, but also the nation state. In almost 20 years concerns have been raised about what single hackers and cyber terrorists can do to a targeted society or individual. In the mainstream media, and our collective weltanschauung, hackers and cyber terrorists have been credited with the ability to create a digital Armageddon or, in American terms, a digital Pearl Harbor. Naturally, the loudest and most graphic contributions to the public sphere have been either news media trying to get our attention or computer software companies in pursuit of marketing their security software. Fear has been the main driving source.

In reality, hackers have not achieved any significant national disturbance or damage to the nation state in the last 20 years. Successful hacker attacks mainly stole information that affected a number of individuals or companies. The few events that targeted the government, such as the highly publicized Wikileaks incident, a massive theft of federal information and communications, did not have any significant long-term impact on the targeted society. The nation state stood unaffected.

Traditionally hackers had little or no interest in destabilizing or challenging the state. The reasoning behind this could be as simple as there is no monetary gain for such activity. Cyber criminality is an enterprise that seeks to earn money through illegal activities and defraud others. That is one reason why fighting cybercrime has had such a low priority as measured by the number of prosecutions. The traditional cybercrime does not threaten the state, the government, or the societal order, and there is no sizeable harm to the general population.

Low Incentive to Attack the State

Cyber criminals are instead avoiding a state confrontation for a simple set of reasons: prosecution, forensics, and ability to extradite. For example, a criminal activity that steals $5 from 100,000 individuals worldwide by using their credit card numbers benefits from the fact that the $5 is still $5 for each victim. Only a few of these 100,000 victims will take their time to fill in a police report or report the crime to federal authorities, because they realize that they probably will not get their $5 back. Unless the federal authorities or credit card companies organize a legal counter activity, the theft of $500,000 goes unpunished. The perpetrators can increase the likelihood that they are never prosecuted or extradited overseas, because the victims are not organized and have no resourceful institutional body to take counteraction. If the cyber criminals instead attack a state, for example, the UK, United States, or France, and create significant damage, the cyber criminals face a forceful counteraction and law enforcement. Until now the aggressors on the Internet have been of minor size and limited resources, but this is changing as states become involved in a militarized cyberspace.

The Militarized Cyberspace

The militarized cyberspace becomes a contested domain when state actors enter in pursuit of an intelligence objective, power maximization, and national security concerns. The main difference now is that there are massive resources available for state actors compared to the earlier generations of independent hackers. States can engage knowledge and ability generation through the defense industry, academic research centers, and covert operations, and outsource the cyber warfare to industrial contractors.

This represents a major shift in the threats. The hackers are no longer a few people operating with a marginal budget in their spare time. Cyber attacks are becoming a well-funded operation, sanctioned from within the defense and intelligence establishment of the attacking country, using allocated resources equal to any military and intelligence operation. This serves as the argument for the comparison, and contrary to the common belief, that the first 20 years of the Internet were more secure than the cyber environment of the future.

The entrance of state actors and the creation of a militarized Internet used as a contested space for intelligence, economic espionage, information operations, and to destabilize adversarial states has radically changed the fundamentals for security in cyberspace. The state actor seeks to exploit weaknesses in the critical national infrastructure and information systems, and take advantage of the fact that our populations rely heavily on the Internet.

One major weakness in the advanced societies is the overemphasis in cyber security training and research on information assurance and the hardening of systems when the paradigm has changed toward full-spectrum cyber operations (Kallberg and Thuraisingham, 2012). By continuously hardening systems a false sense of control and security is maintained, mainly based on the earlier attacker profile with single individual or small criminal efforts to penetrate the system. Other security concerns related to cyberspace such as influencing population sentiment, information operations, and destabilizing governments by systematic attack are unaddressed. Cyber security now consists of tools and the implementation of those tools and lacks abstract theory, therefore, becoming incoherent and lacking a strategic societal system approach. This gap of consistency is an inlet for attacks.

The Growing Cyber Opportunity

The state acts in the state's best interest, unless it is confused by media. In the last decade the national security debate has oftentimes missed the distinction between national security and individual security. The attack on the World Trade Center in New York added fuel to an already established popular notion that attacks on a number of individuals are an attack on the state. Terrorism is a menace and it is the state's responsibility, as the state claims the right to maintain the monopoly on violence, to protect the citizens of the state. The blurred demarcation between national security and individual security becomes apparent for a cyber-defending nation. Cyber attacks, seen from a state perspective, are annoying and a threat to the economy until it reaches a point when it becomes a national security concern. The United States considers an attack on military networks, critical infrastructure, and main industries as an attack on the state itself.

As cyberspace matures, states are able to define their reasoning and level of thresholds for national security response. Over the last few years there has been a shift in cyber strategy focusing on the national security. During the next decade the national security concerns in cyberspace are likely to override the earlier paradigm of focusing on securing individuals and single corporations. The attacks on individuals and corporations have become solely a criminalized act; meanwhile, the state considers attacks on the national critical infrastructure, the state's core function, the state's legitimacy and authority, and its military complex as attacks on the state itself.

The increased reliance on computer networks, changes in societal sentiment influenced by the Internet, and the increased complexity create opportunities for an aggressor and terrorists. It is unlikely that terrorists will be able to represent a permanent cyber threat to a nation due to the cost and infrastructure needed. The combination of a covert state actor and terrorists as executors of attacks creates a different more likely scenario for the future.

Covert Operations by Proxies

The scenario becomes more complex if a state actor gathers information about cyber vulnerabilities in the networks of a targeted organization or other nation and then outsources the attack to a criminal or terrorist network. This innovative modus operandi creates numerous obstacles and considerations for the targeted organization. First, the attribution problem is highlighted, because even if the executing criminal network is identified, it is still unclear which actor initiated the attack. Criminal networks are enterprises and the compensation could be a range of illicit goods (Kan, 2009). States can pay to get things done. If necessary, a covert operating state can pay criminal networks cash, drugs, weapons, or any currency to act as a proxy. Terrorist organizations can finance their operation through cyber terrorism "entrepreneurship" instead of engaging in other forms of financing that are far riskier for detection such as drug dealing and credit card fraud. Second, the lack of attribution evaporates the option to initiate retribution against the initial attacker. Third, it is likely that the vehicles for the attack are dismantled directly after the attack. The computers and networks that were used for the attack are no longer in use afterward. The lack of attribution removes the risk to engage and the fundamentals of state-to-state deterrence are no longer in place (Reed, 1975).

Cyber terrorists can be a national security threat, and create significant damage to critical infrastructure and national assets for the targeted state, if the terrorists are given the toolset and pre-attack intelligence from a state actor. The covert warfare in cyberspace in many cases resembles the covert operations in the Cold War. The targeted country, or organization, could assume where the attack is coming from but attribution is not strong enough for retribution. A state engaging in retribution toward another state could face other grave unanticipated political consequences, which pose uncertainty and generate a risk-averse state actor.

The aggressor's risk is lowered if the state actor collects vulnerabilities in the opposing state's networks, builds cyber weapons, and creates a strategy to create disruption and destabilization in the opponent's networks, but uses a proxy to carry out the actual attack. In this case the aggressor is unlikely to be held accountable for its actions. The opportunity not to be held accountable is extremely inviting for countries that are covert adversaries.

If the adversary is skilled, it is more likely the attribution investigation will end with a set of spoofed innocent actors whose digital identities have been exploited in the attack rather than attribution to the real perpetrator. A strong suspicion would impact interstate relations, but full attribution and traceability are needed to create a case for reprisal and retaliation. Attribution can be graduated, and the level varies as to what would be accepted as an "attributed" attack. The national leadership can accept a lower level of tangible attribution, based on earlier intelligence reports and adversarial modus operandi, than the international community might demand, but it is restrained in taking action.

La Raison d'état

Cyberspace is already by definitions and doctrine a war-fighting domain even if only a few states are able to do any offensive cyber operations, but the strategic abilities will grow in the next decade. There are several reasons why cyber weapons are inviting.

In an era of austerity countries seek alternatives to traditional military policy options that are better suited for future conflicts, but also reduce the collateral damage that a kinetic operations creates. The pursuit of cyber abilities also drills down to pure financial numbers (Kallberg and Lowther, 2012). Militaries are expensive and require a standing force to ensure ability and deterrence. If the force is a professional army it will cost to recruit, train, pay, and pension its soldiers. In modern state reasoning, cyber warfare is a cheaper option for both covert operations and to engage and destabilize an adversary (Kallberg and Lowther, 2012).

States act in their own self-interest; therefore, it is questionable if a regulated cyberspace is in the long-term interest of the major powers, as a restrictive use of cyberspace would undermine their dominant status. Earlier efforts to create a uniform approach toward information technology security on a global scale have shown marginal progress. One example is the global standard for security certification of hardware, "Common Criteria," that has been hindered by the lack of unrestricted trust between nations (Kallberg, 2012a). If any international effort fails to create a uniform approach to securing the Internet domain we can assume by logic that major actors prefer the anarchy before order because there is a perceived opportunity and potential future gain for these powers.

Expanded Reach for Cyber Conflicts

State actors will implement cyber conflict at all levels that benefit the state. As an example, targets that had limited value for cyber criminals, such as the global space-borne information grid, are a prime target for a state actor (Kallberg, 2012b). Satellites are a major concern for any state or nonstate actor who intends to conduct operations in secrecy. Satellites gather intelligence, provide surveillance, and perform reconnaissance (Moltz, 2011). This can be extremely annoying to states that seek to avoid transparency between their international commitments, their public posture, and their actions behind the scenes.

Terrestrial cyber attacks are a single exploit on thousands, if not millions, of identical systems, and the exploit will be eliminated afterward by updates or upgrades. The difference between satellites and terrestrial cyber exploits is that a satellite is often custom made, whereas the computing design is proprietary. Cyber attacks in space exploit a single system, or limited group of systems, within a larger group of satellites (*Wired*, 2011). These space-borne assets have a variety of operating systems, embedded software, and designs from disparate technological legacies. As more nations engage in launching satellites with a variety of technical sophistication, the risk for hijacking and manipulation through covert activity increases. A satellite's onboard computer can allow reconfiguration and software updates, which increase its vulnerability to cyber attacks. The attack on the satellite is tailored, one shot, and unique.

An attributed cyber attack on the global information grid would be considered an act of war, and provide the targeted state with at least a theoretical *casus belli*, a risk that the aggressor would seek to avoid. An act of war is a tangible security risk that can have catastrophic consequences for an aggressor nation. Are attacks on the global information grid ideal for being outsourced from the aggressive state actor to terrorists and criminal network to avoid attribution? The symbiosis between a state actor and cyber terrorist can provide an ability that makes cyber terrorism a tangible national security threat at the strategic level.

CONCLUSION

The threat from cyber operations will increase in the next decade, even if we have implemented extensive information security. The Internet and the application layer become a globally contested domain where the entrance of state actors as contestants and aggressors create a radical shift. The early hackers and information thieves had limited resources and mainly a financial goal. State-run operations have a complete different set of targets and goals.

If states collect vulnerabilities in targeted systems, utilize the whole covert spectrum, and instead of attacking themselves uses terrorist groups as proxies, then cyber terrorism is a tangible and relevant national security threat.

The digital environment where critical assets can be copied, sent, and forwarded within seconds, ushers in a symbiosis between aggressive adversarial state actors and terrorist networks when the state actor can produce military-grade cyber weapons for the terrorists to use. Waltz (1990) argued that the power embedded in nuclear arms is not what you do but what you can do. The outsourced proxy cyber war from state actor to cyber terrorists operates along the same lines as military-grade cyber weapons dispersed to violent groups and militant political groups create extensive uncertainty. This uncertainty is based on what an aggressor can do— not what they actually do.

This development creates an asymmetric covert conflict with an anonymous aggressor and a reactive targeted society. Terrorists can reach their objectives, create damage, influence policy, and leverage the disproportional power relation between terrorists and the defending state.