The Proliferation of Weapons in Cyberspace

Daniel Cohen and Aviv Rotbart

Introduction

Cyberspace is a phenomenon whose fundamental nature is to utilize an electromagnetic field for human purposes by means of technology. This article argues that such technology is a type of weapon. A common dictionary definition of "weapon" is "any instrument used in combat" or "any means employed to get the better of another."[1] A "cyber weapon," therefore, is one that strikes with the purpose of vanquishing another by attacking systems connected to cyberspace. Cyber weapons can be used as non-lethal weapons and have the ability to cause tremendous destruction and serious damage without destroying physical infrastructures or human life. The cyber-strategic environment includes the use of cyber weapons in order to penetrate the enemy's systems for purposes of espionage, psychological warfare, deterrence, and damage to information technology systems or physical targets.

We distinguish between the broad and prolonged capability to attack strategic targets that have a high degree of defensive capability and an attack that is liable to cause local or temporary damage. Currently, offensive capability of the former kind is restricted to a limited number of states, and requires major resources. In contrast, the latter type of capability costs little, and consequently, there are already signs that weapons are being mass produced, are available on the open market, and are used by terrorist and criminal organizations.

Cyber warfare is rapidly becoming one of the popular offensive methods used by states seeking to protect their interests from hostile states

Daniel Cohen is the coordinator of the Military and Strategic Affairs Program at INSS. Aviv Rotbart is a Neubauer research fellow at INSS.

or organizations. This is apparent in the recent cyber attacks covered by the media, such as the attack, attributed to Iran, on oil companies in the Persian Gulf and on American banks; or the attacks on Iran's nuclear facilities, attributed to the United States and Israel.[2] There are a number of reasons for this, including the ability to carry out a targeted attack, the attacker's ability to camouflage itself, and the victim's ability to conceal the incident, thus avoiding the need to strike back. Cyberspace allows states with resources and high level technological capabilities to employ an arsenal of weapons for a cyber attack. Similarly, states lacking resources can also equip themselves with offensive weapons and operate in cyberspace, although on a more limited scale and with less potential for damage.

A unique aspect of cyberspace not found in other arenas of combat is the ability to defend against viruses or other malicious codes[3] that have already been used in the past and discovered by security bodies.[4] Ostensibly, cyber weapons can be used only once, as they become useless the moment they are identified and signed.[5]

That said, do all the man-years invested in developing sophisticated malicious codes go down the drain as soon as an attack is discovered and signed? This article shows that they do not. As cyber attacks increase, cyber tools and capabilities proliferate around the world. One of the main reasons for this is that cyber weapons, for example, malicious code used in one attack, can be used for other attacks as well after they are converted. In a term borrowed from the world of biology, this is called "mutated code." Such code has functional characteristics similar to the original code from which it was created (and can even be totally identical). The difference between the original code and the mutated code is syntactical (structural) only and not semantic, where it is intended to evade the radar of software that identifies attackers.

From this we can conclude that if malicious code falls into the hands of an adversary with motivation and capability, it provides the attacked party with a weapon that, if it arms itself appropriately while executing complex actions such as reverse engineering, can be exploited for repeated use.[6] In addition, an attacker who understands the weapon can use it effectively and change it according to his needs to carry out further attacks.

We are in the throes of a silent cyber war, and while very few details have been leaked to the media, the mystery cannot be maintained forever. Consider, for example, the development of the field of unmanned aerial

vehicles, or drones. In its early days, the field was cloaked in secrecy. Few states had the ability to operate drones for espionage and subsequently for attack, and they made calculated and careful use of the technology in order not to reveal it to their adversaries. With the increasing use of unmanned tools, the wall of mystery has been breached, and today, thanks to the media, detailed descriptions of the countries that use drones, the targets of this type of attack, and drones capabilities and limitations are available. Terrorist organizations too have closely studied the new-old weapons that states use against them, and have developed means of defending themselves.

Another result of the extensive use of drones and the resulting media exposure is that an arms race has commenced, with many countries attempting to join the exclusive club of those in possession of these weapons for espionage and offensive purposes.[7] State supporters of terrorism have also entered the race, and terrorist organizations operating under the sponsorship of these states also enjoy the fruits of the investment. For example, Iran has acquired the ability to operate drones, and it did not take long for this capability to make its way to the Hamas and Hizbollah terrorist organizations.[8]

According to estimates, only a limited number of states currently possess the ability to carry out an attack in cyberspace in order to disrupt industrial control systems and cause physical damage, as with the Stuxnet virus, which damaged the centrifuges in the Iranian nuclear reactors, and many other states have joined the race to achieve this capability. Thus, a new type of combat weapon is being acquired for the purpose of causing damage and destruction from a great distance.

Carrying out an attack that will damage an industrial process is not overly complex, and it can be perpetrated by junior engineers. In contrast, understanding the industrial process that occurs at the target under attack and performing an in-depth analysis of it requires the full intelligence and penetration capabilities of a state.

Non-state actors in cyberspace, particularly criminal and terrorist organizations, can make use of, or already have made use of, variations of existing malicious codes and convert them so as to serve the organization's purposes. This is what happened in 2012 when criminal organizations made their own changes to two existing viruses, Zeus and SpyEye, and

managed to withdraw some 78 million dollars from banks around the world.[9]

The greater the accessibility of existing codes and the greater the ability of individuals or small organizations to perform conversions and modifications, the greater the proliferation of malicious codes for attacks on the financial world and for economic gain for criminal organizations. Furthermore, these codes will also spread to terrorist organizations that wish to accomplish social, ideological, and political goals through intimidation and the disruption of normal civilian life.

Capabilities of Actors in Cyberspace

The transition from the industrial age to the information age has produced a new product in the shape of cyberspace. The development of the information age is connected to the growth of communications, control, and computer technologies, which have deep social and economic significance. The year 2008 has symbolic significance in that it was the year in which, for the first time, the number of home computers (most of them connected to the internet) passed the billion mark. That same year, it was reported that the number of people in the world possessing cell phones exceeded the number of people without cell phones. Every such computer or phone can serve as a gateway to cyberspace and a weapon for a potential attacker (or itself become a target for attack).[10]

The rapid technological developments of the information age create unique characteristics and features in cyberspace that make it possible to work quickly against adversaries located far from the attacker. These developments may also change the face of the modern battlefield, creating theaters of combat in which the non-state actor is the main actor and exerts its influence on the policy of governments and international institutions to a greater extent than in the past. For example, the fighting in Kosovo between 1996 and 1999 was dubbed "the first internet war." State and non-state actors used the internet to disseminate information and propaganda and to demonize their adversaries. Hackers used the internet during the fighting as a tool against both other former Yugoslavia states and NATO, interfering with government computer systems and taking over government websites. Individuals and activists used the web to disseminate messages from the combat zone.[11]

Another example can be found in the attacks in Estonia. Commencing in April 2007, Estonia was attacked for three weeks with a DDoS, or distributed denial of service. The wave of attacks targeted the websites of government institutions, banks, and newspapers. Since it began after a clash with Russia over demonstrations by the Russian minority in Estonia, Estonian and NATO officials hinted that there had been Russian state intervention in carrying out the attacks.[12]

Cyberspace has broad significance with regard to the use of military force, terrorist activity, organized crime, espionage, and intelligence. Concerning the use of force, an attack on computers does not require a state base; it can be carried out by organizations and even individuals. In addition, a cyber attack can also be perpetrated between friendly states competing for diplomatic and economic intelligence.

A unique trait of cyber warfare is the ability of both attacker and victim to conceal almost perfectly the fact that an attack did indeed take place. Because of the nature of cyberspace, the attacker can carry out the offensive action at a great distance from the target and use concealment techniques to prevent exposure almost entirely. The victim, for its part, can always claim that the damage to its systems was the result of a hardware or software problem, thereby avoiding tarnishing its image and responding or threatening to respond.

A direct result of the ability to hide in cyberspace is very limited media exposure of attacks. From the little that is published in the press, however, we can see an increase in the number and sophistication of cyber attacks. All the major powers are already involved in cyber warfare in one way or another, and many other countries are investing in developing attacks and defense capabilities in cyberspace.[13] Cyber warfare is being perfectly integrated into the new "Cold War" that is underway between East and West because it allows the adversary to be threatened or harmed without compelling it to respond. A cyber attack that is not reported and for which no one claims responsibility is an attack to which the victim does not feel obligated to respond; nonetheless, it is totally cognizant of the hint sent by the attacker. This is the essence of a cold war.

On the defensive side, with the expanded use of cyber weapons, there is greater awareness of the dangers of these weapons and the potential damage they can wreak in terms of security, economics, and image. As a result of this awareness, more resources are being invested in developing

software systems that are better protected and more secure, as well as in securing facilities and critical infrastructures in various countries. As in any battle between attackers and defenders, in cyberspace too the attackers had the upper hand when cyber warfare began to develop. Now, however, it appears that the gap is narrowing, as more and more organizations are working to secure their IT infrastructures.

One of the characteristics of cyberspace is the difficulty in identifying the attacker. This contrasts, for example, with the attack on Pearl Harbor by Japanese Imperial Air Force bombers in 1941, which led the United States to declare war on Japan. After the large cyber attack such as that on Aramco in August 2012, the identity of the attacker is still being debated by security experts, even though an accusatory finger is being pointed at a state actor (Iran).[14] The characteristics of cyberspace also make it difficult to distinguish between intentional harm and a glitch, and to attribute an operation to a particular actor, thereby making it problematic for victims to respond to an attack. Some people argue that the characteristics of cyberspace today are still more advantageous for the attacker than for the defender.[15]

Groups that Employ Cyber Attack Tools

There are five main groups that employ cyber attack tools today or have the potential to use them in the future.[16]

States develop offensive and defensive capabilities as part of their exercise of power. Reasonable estimates are that some 40 states are acquiring cyber warfare capabilities or have already acquired them, including the ability to carry out cyber attacks. Most of the national programs are covert, and there is no consensus on the extent to which existing international law, which is valid for an armed conflict, is supposed to apply to this new type of attack.[17]

In the information age, there is increasing state intervention in the economy, civilian infrastructures, national security, civilian security, inter-organizational communication, management of government institutions, education, and so forth. As a result, countries around the world are increasing their investment in the defense of computerized systems, which is reflected in the resources allocated to the issue and to the development of specialized technologies and security concepts.[18] At the same time, defense and intelligence agencies are adopting the tools of cyberspace in order

to achieve their goals. Information technologies are also providing state intelligence services with a wide range of ways and means to perform the task. States have the ability to gain access to closed computer systems by infiltrating or activating an agent and by intervening in the supply system and introducing "infected" components into the enemy target.

The same characteristics of cyberspace that make it difficult to identify the attacker can also provide the attacking state with an advantage by utilizing a proxy to carry out an attack or take responsibility for attacking a state or a business enterprise in a rival country.

For example, in state cyberspace, three new programs that employ malicious code were exposed in 2012: Flame, Gauss, and miniFlame. Flame is an example of complex malware that existed undetected for some time, and collected data and information. At 20 MB, Flame is a large program for a virus, as most viruses rely on their small size to avoid detection. The program includes properties of a Trojan horse, allowing those who activate it to open a "back door" to computer systems in order to collect information and pass it to remote servers around the world. In addition, Flame is capable of recording audio by means of the computer's microphones, of taking screen shots, and of connecting to Bluetooth devices in the area of the attack.

This type of attack, which, because of its complexity is attributed to a state, affects not only government institutions, but also businesses and the infrastructures of business enterprises that have ties with government institutions.[19]

Criminal organizations are driven mainly by criminal and business interests. Organized crime uses hackers for profit: identity theft, fraud, spam, pornography, concealment of criminal activity, money laundering, and the like. Some 80 percent of internet crime is perpetrated by criminal organizations.[20]

Former Interpol president Khoo Boon Hui claimed that banks in the United States are losing 900 million dollars every year as a result of computer crime.[21] During the first quarter of 2012, it was reported that criminal organizations had created variations of SpyEye and Zeus for an attack on banks in Europe and the United States. The attack was first identified in Italy, where the code was tailored specifically to attack different banks. Later, a similar type of attack was identified against German and Dutch banks. The attacks then spread to Latin America and the United States.

The attackers managed to steal at least 78 million dollars in transfers from the accounts of some 60 financial institutions.[22]

According to the assessment of senior analysts, hackers manage to steal about one billion dollars a year from financial institutions. There are those who estimate that three of the major crime gangs operating in this field have succeeded in stealing some 100 million dollars a year by means of computer systems, while according to the FBI, in 2010, only 43 million dollars were stolen from American banks by non-cyber methods.[23]

Business enterprises mainly operate defensively since the scope of cyber attacks in the business context is growing significantly. However, some of them could elect to attack competitors for the purpose of industrial espionage – or have already done so. In addition, business enterprises face technological challenges in cyber defense such as protecting online payments, video broadcasts in real time, smartphone apps, and many others.

Terrorist organizations exploit the advantages of using cyberspace in order to pass coded messages, recruit supporters, acquire targets, gather intelligence, conceal operations, and the like. Out of cost-benefit considerations, terrorist organizations also use cyberspace to carry out cyber attacks, which help them influence public opinion so as to convey political messages and create demoralization and intimidation in order to disrupt citizens' lives. Terrorist organizations focus their offensive cyber operations on symbols of power such as the websites of government and media institutions.

One of the first documented attacks by a terrorist organization against state computer systems was carried out in Sri Lanka by the Tamil Tigers guerrilla fighters in 1998. For two weeks, Sri Lankan embassies around the world were flooded with some 800 e-mails per day saying, "We are the internet Black Tigers and we're doing this to disrupt your communications."[24] Some argue that this message induced fear at the embassies.[25] In Israel in January 2012, a group of pro-Palestinian hackers calling themselves "Nightmare" brought down the websites of the Tel Aviv Stock Exchange and El Al Airlines for a short time, and disrupted activity on the website of the First International Bank of Israel. Referring to this hacking incident, a Hamas spokesman in the Gaza Strip announced that the organization had initiated a new field of resistance against the Israeli occupation.[26]

Finally, *anarchists*, who oppose the existing institutional system, are eager to sabotage it from within or without, and will seek to attack the computer systems that are the basis for running it in order to disrupt and even destroy the social order and the fabric of life in the country. For example, groups of activists or individuals could attack websites in order to plant a political message, or endeavor to breach censorship mechanisms and reveal secrets.

In November 2012, during Operation Pillar of Defense in Gaza, government officials in Israel announced that there had been 100 million attempted cyber attacks against Israeli government internet services.[27] Anonymous, an organization that represents a theoretical concept of a community of hackers and activists, took responsibility for bringing down Israeli websites and leaking the credit card numbers of Israeli citizens during the conflict. Anonymous also published a list of more than 650 Israeli websites that it claimed were taken down or defaced as a result of the attacks by "hacktivists."[28]

A US government official has stated that "a couple dozen talented programmers wearing flip-flops and drinking Red Bull can do a lot of damage."[29] However, the ability to attack strategic targets of an enemy with advanced defensive capabilities differs from the ability to cause local, tactical damage. The various actors are acquiring cyber weapons in accordance with their capabilities and their limitations with regard to setting up a cyber force with offensive capabilities, and this has also been influenced by the interests and needs of each actor.

Table 1 charts cyber weapon capabilities of the various actors. Currently, there is a limited number of states with the capabilities and high level technological resources with the ability to use cyber weapons to attack both physical and cyber strategic targets. However, there is a low threshold of entry, and there are cyber weapons with the ability to cause tactical damage. Such weapons can be mass produced quickly and at a relatively low cost, and some of them are even available on the open market. States exploit cyberspace in order to gain an advantage and to promote their interests by collecting information, achieving the capacity to strike at the capabilities of anyone considered an enemy, and so forth. Non-state actors such as terrorist and criminal organizations can also leverage cyberspace for their purposes, and they benefit because it affords small actors influence that is disproportionate to their size.

Table 1. Basket of Cyber Weapon Capabilities of the Various Actors in Cyberspace

	Use of cyber weapons to attack physical equipment	Use of cyber weapons to attack in cyberspace	Use of cyber weapons for espionage	Denial of service and psychological warfare
States	Because of the large resources required, only a limited number of states today have the ability to carry out a cyber attack that causes physical damage to the defender. (According to reasonable estimates, the United States, Israel, Russia, China, and Britain have this capability.) Many other states are attempting to reach the threshold of physical attack capability or are keen to do so.	Medium-sized resources are required for this, and the number of states with electronic attack capabilities is greater than the number with the ability to attack physical equipment. States can carry out an electronic attack and/or use proxies to carry out such an attack.	The leading states in the field of industrial espionage and espionage for intelligence gathering are Russia and China, and, according to some, the United States and Israel. Since large resources are needed to make use of this capability, only a limited number of states possess it. If we assume that espionage is the second oldest profession in the world and that most states engage in espionage in one way or another, spyware to be used on targets inside and outside the country will become more common as access to technologies that provide cyber espionage capabilities increases.	This capability is relatively simple, and any state is likely to use it during a conflict with another state or by means of proxies.

	Use of cyber weapons to attack physical equipment	Use of cyber weapons to attack in cyberspace	Use of cyber weapons for espionage	Denial of service and psychological warfare
Terrorist organizations	Terrorist organizations today lack the resources required to realize this capability. Nevertheless, there are states that use terrorist organizations to carry out terrorist attacks, and it is therefore not inconceivable that they have been used or will be used to carry out physical cyber attacks as well.	Terrorist organizations lack the resources required to realize this capability, other than those acting as a proxy for a state.	Large resources are required to realize this capability. However, since it is one of the needs of terrorist organizations, they might attempt to acquire it (even though ostensibly, this weapon requires resources that are relatively complicated to acquire).	Used by terrorist organizations in order to disrupt routine life and sow anxiety and panic among civilians.
Criminal organizations		Used by criminal organizations in order to perpetrate financial crimes and extort business organizations and the wealthy.	Carry out the espionage activities necessary to perpetrate other crimes: identity theft, credit cards.	
Business organizations			Today, spyware is used to provide a business with an edge over a competitor.	A capability that can be exploited to harm competitors – for example, by bringing down a competitor's website or service.
Anarchists				A capability used by activists to convey messages by disrupting governmental and civilian systems.

The table shows that the state actor is capable of achieving offensive capabilities in all categories. States have diverse needs such as espionage and damaging industries in an enemy state. States also have restraints such as avoiding harm to innocents and avoiding a great deal of environmental damage. This leads to the development of cyber weapons for cyber attacks rather than physical attacks, or weapons for a psychological attack such as a warning before a bombing that makes it possible to avoid harming civilians.

The other actors in cyberspace have more focused interests and needs: terrorist organizations have more limited capabilities and resources, and are driven by the desire to accomplish political and ideological goals by means of damage to physical systems (even though no such incident has yet taken place), espionage, or psychological warfare. Business organizations, in contrast, are interested mainly in industrial espionage, and sometimes also in disrupting the activities of their competitors. Criminal organizations are interested primarily in obtaining assets and money fraudulently, and therefore focus on attacking cyber systems and on espionage that supports such activity (collecting credit cards and identity-linked information for an attack).

The Threat of the Repeated Use of Cyber Weapons

Every new cyber attack that is revealed brings cyber weapons closer to belonging to the public domain. As the use of cyber warfare tools increases, it is not inconceivable that more sophisticated cyber weapons with the ability to cause strategic damage will become commonplace, with various versions finding their way into the hands of state sponsors of terrorism and terrorist organizations.[30] An example of this is the Stuxnet virus attack on Iranian nuclear facilities. The attack continued in secret for several years, but the moment it was discovered, it led to the in-depth study and analysis of the virus's code and an attempt to understand everything that enabled it to be successful. The results of the analysis could have been used immediately to develop new viruses based on similar principles. The secret was exposed and the weapon disseminated. Theoretically, an analysis of malicious code by security companies and security experts could divulge the virus to various actors, ranging from states to terrorist organizations. Cyber weapons will not always remain the province of the few.

There is a belief that cyber weapons can be used only once, and that this will restrain their use and retard the development of new cyber warfare tools

because it is imperative to innovate constantly and to avoid using weapons that have already been discovered and signed by protection software. This belief has not proven itself; in fact, the opposite is usually the case. In other words, there is widespread repeated use of cyber warfare tools, which undergo changes to allow them to evade the radar of protection software. Cyber attacks depend on successful exploitation of a vulnerability in the system attacked.[31] The vulnerability can reside in a software component whose code was written without sufficient attention being paid to security, in a hardware component that can be penetrated and programmed to carry out destructive actions, or in a non-secure communications protocol.

In order for a system to be considered secure, all the aspects noted must be checked and secured separately. The only thing that is required in order to penetrate and take over the entire system is a small breach in one of them. Let us suppose, for example, that there is a website that contains sensitive information and is very highly secured, so that it is not vulnerable to attacks such as XSS, SQL Injection, and the like. Let us also suppose that there is another website, unimportant and totally unsecured, on the same server on which this secure site is located. In such a case, an attack can be launched on the other site, meaning that the computer where the sites are stored can be accessed through it. Once the computer has been taken over, none of the systems protecting the secure site are relevant any longer, and the secure site is compromised.

While cyber weapons that have been discovered and signed are blocked from being used in their original form, this is still a far cry from blocking them totally and rendering all the code that was developed irrelevant. First, every offensive weapon is composed of a number of modules (software components), including the module responsible for concealing the weapon in the attacked system, various information-gathering modules, an information-storage module, and a module for sending information to the command and control servers of the weapon. If a Trojan horse is discovered and signed, some of its modules can be reused by incorporating them in the code of another Trojan horse. Such a combination creates a new attack weapon that is likely to evade the radar of the anti-virus systems. Another way to reuse malicious code is by concealing it using methods known in the world of software as obfuscation[32] and packing.[33] These can sometimes change the malicious code so that it will not be discovered by protection software. Finally, even if the code that has been discovered

cannot be reused, a mutated code, which is based on similar ideas and methods of operation and exploits the same vulnerabilities as the original code, can be developed.

This claim is supported by the use of different variations of the Flame virus, which has recently been publicized in the media. Even after the original virus was discovered, various derivatives of it continued to attack the target computers until they were discovered.[34] Stuxnet, which is considered the most sophisticated virus discovered up to this point, opened the door for many others that imitate its modes of operation.[35] In fact, we can say with a high degree of probability that Flame and Stuxnet combined demonstrate in the clearest manner the ability to reuse malicious code because they have a large amount of code in common.[36] Although they were designed for completely different purposes (espionage and causing damage to industrial control systems, respectively), there are a number of functions that both must fulfill. These are penetrating the organization's computer system, concealing the existence of the weapon, analyzing the organization's network, and propagating within the network in order to find valuable target computers. Both weapons can carry out these functionalities by using the same code, which was written and checked only once.

Since the process of producing cyber weapons is long and expensive, the advantages of being able to use the same code for two different tools are enormous. However, this is a process that does not guarantee a positive result, despite the amount of effort that has been expended on it. Furthermore, even when a vulnerability is discovered, in order to exploit it and use it to penetrate the computer system, a great deal more work is required to write the appropriate code and build the files that can take advantage of the vulnerability.[37] It is also possible that no way will be found to do so because of the complexity of the vulnerability, and then further research will be necessary so as to identify another vulnerability that is easier to exploit. Therefore, when a creator of cyber weapons develops the ability to penetrate a system, his intention is to exploit it in several different scenarios and with several different tools in order to maximize the profit from his investment. However, the greater and more varied the use of a particular secret capability, the greater the chances that it will be exposed and blocked. This is a restraining factor in the considerations of

the cyber weapon creator with regard to propagating the tools and using the capability in other scenarios.

On the face of it, it might be expected that after malware is discovered and the existence and exploitation of the vulnerabilities become public, the programs in which the vulnerabilities were discovered (for example, Windows Operating System) would be updated immediately and the update sent to every computer on which the system is installed, thereby rendering all computers immune to the malicious code that exploits the vulnerabilities in question. This is not what happens, however. The process of protecting systems from malicious code that has been discovered comprises four main stages: discovering the vulnerability exploited by the code; closing the gap in the system; distributing a security patch to all users of the software; and only then installing it on all computers. Closing the gap through which the malicious code infiltrated the system is complex because after this is done, the programmers must also make sure that the performance of the system has not been affected by the change that has been made. The effects of the change must be carefully examined and various test scenarios run in order to make sure that the problem has been resolved. Depending on the complexity of the system, the process could take many weeks or even months.

Furthermore, even after a security update (patch) has been developed and distributed, many people do not update their computers automatically; this is especially true of companies that have an internal communication network that is not connected to the internet. In such cases, computers on the internal network will be updated only after the individual in charge of security acquires the software update or patch from the internet in order to perform the update. For these reasons, vulnerabilities can be exploited long after they have been discovered and publicized.

There is an interesting catch-22 phenomenon associated with security updates. When Microsoft, for example, encounters a security problem in its operating system, it develops a security update and seeks to provide it to all users who have been exposed to the problem. However, the moment the update is distributed, hackers and writers of malicious code become aware of its existence. They can analyze it in order to understand which security problem it solves, and then write malicious code that exploits the security gap that Microsoft itself has revealed. Of course, the malicious code can work only in systems on which the security update has not yet been

installed, but surprisingly, there are quite a few like that, belonging not only to private users who do not bother to update their computers frequently but also, and particularly, to companies whose computer personnel are responsible for taking action in order to update the company's computer system. This creates a window of several days or more during which the hackers can exploit the security gaps before they are closed.

The scenario described above is an example of the reuse of malicious code that is facilitated by the abuse of the security update distribution process. In general, Microsoft distributes security updates for its programs on the second Tuesday of each month, and this is called "Patch Tuesday."[38] The following day is called "Exploit Wednesday," because hackers analyze the security updates and begin to exploit them in order to penetrate computers that have still not been updated.

The ability to create new cyber weapons based on existing weapons or on a vulnerability that has been publicized is not always that simple and immediate. Hackers who exploit Microsoft's security updates in order to discover vulnerabilities in Windows must invest time in analyzing the patch and comparing the files that it corrects with the original files in order to identify where exactly the corrections have been made, since that is where the vulnerability lies. Finally, they must also find a way to exploit that vulnerability. This process can take anywhere from days to weeks, depending on the complexity of the patch and the determination of the hacker.

In contrast, an in-depth analysis of a sophisticated tool such as Flame would require more time and more professional and experienced personnel. In general, such an analysis is performed by states or security companies rather than by private individuals. An example is the cyber weapon, MiniFlame, which was analyzed in depth by the internet security firm, Kaspersky Lab.[39] This analysis, which took several months and required a large amount of manpower, was performed in order to develop protection against the weapon and to distribute it to the company's customers. However, the products of the analysis could serve as a basis for mutated code that utilizes similar techniques and sometimes even part of the code from the original cyber weapon. If these products were to leak from Kaspersky Labs to cyber weapon developers, it would not be surprising to discover new tools that share code with MiniFlame but are

used by other attackers against other targets, and possibly even against the original creator of the weapon, in a boomerang effect.

In recent years, there has been an increase in cyber attacks that require broad and prolonged offensive capability against strategic targets with a high level of defensive capability. Only a few states have this capability today, but it is not inconceivable that this trend will persist and that other states will achieve such capabilities for both defensive and offensive purposes. The trend is also evident in the global cyber crime market.[40] In Russia, for example, there are signs indicating that organized crime organizations have begun to join forces to increase their profits by sharing data and tools.[41] The Kaspersky Lab's 2012 Security Bulletin revealed that the number of malicious code attacks on the internet among the company's clients almost doubled between 2011 and 2012 (from 946,393,693 attacks in 2011 to 1,595,587,670 in 2012). These attacks took place in 202 countries. Criminal organizations used 6,537,320 unique domains as tools for perpetrating financial attacks, some 2.5 million more than in 2011.[42]

Conclusion

Many states and non-state actors are participants in a secret arms race in cyberspace. The map of interests of the various actors indicates that different kinds of attacks in cyberspace require state actors to be prepared for a range of possible attacks. At the same time, characteristics and properties of the cyber battlefield pose dilemmas for the attacker. Cyber weapons are reusable. When an attacker uses them, it reveals its capabilities to the victim, who can then reuse them, possibly even against the attacker itself (the boomerang effect). Weapons with strategic destruction capability, such as Stuxnet, are liable to fall, or have already fallen, into the hands of terror-supporting states and terrorist and criminal organizations, and will serve as a basis for cyber attacks. Independent development of cyber attack weapons or their purchase on the black market is liable to provide these elements with the ability to cause widespread damage, even if the tools obtained in this way do not reach the level of sophistication of the cyber weapons created by advanced states.

Both the possession of cyber weapons by private entities and the resulting uncontrolled proliferation are problematic. For example, a senior security researcher claimed that Stuxnet's code is found online – and even offered to share it with others.[43] On another occasion, an expert who had

analyzed Stuxnet claimed that the code was equivalent to a powerful weapon, but when asked why he did not destroy the copy in his possession, he preferred not to answer.

Aside from a discussion of ethical and moral questions, we believe that it is appropriate to implement both an intra-state and an international arrangement with regard to this issue in order to activate the regulation and enforcement mechanisms against proliferation of malicious code. Consideration should be given to limiting, and in certain cases, even banning, the possession of malicious computer codes so that they do not fall into the wrong hands. On this subject, we can perhaps learn from the war that is being waged against the illegal distribution of copyrighted intellectual property such as films and music.

Today, the arsenal of cyber weapons with the ability to cause tactical damage is reducing the procurement gap between states and non-state actors. Conversely, the gap between states with an arsenal of offensive capabilities against strategic targets on the one hand and states and actors that do not have the ability to achieve the high threshold for entry on the other is growing. It is not inconceivable that states and other actors will pursue the acquisition of cyber weapons that can cause physical damage, and there must be means of dealing with the dramatic increase in threats in cyberspace. Thus, there is an urgent need to discuss the concept of reusable cyber weapons that can be exploited for other attacks.

Notes

1 The American Heritage Dictionary of the English Language.

2 Mark Ambinder, "Did America's Cyber Attack on Iran Make Us More Vulnerable?" *The Atlantic*, June 5, 2012, http://www.theatlantic.com/national/archive/2012/06/did-americas-cyber-attack-on-iran-make-us-more-vulnerable/258120/.

3 Computer codes written for the purpose of carrying out an action on a computer system, usually data theft or the disruption of processes in the system, which is run without the knowledge or approval of the system's owner.

4 For example, when a malicious program is discovered by an anti-virus company, an electronic signature of the virus is created and sent to all the company's clients. This way, when another client is attacked by the same virus, the anti-virus program will identify the attack by the signature and block it effectively.

5 Shmuel Even and David Siman-Tov, *Cyber Warfare: Concepts and Strategic Trends*, Memorandum No. 117 (Tel Aviv: Institute for National Security Studies, May 2012).

6 The process of discovering the technological and engineering principles of a product by analyzing its structure and modus operandi. Generally, this process includes dismantling the product and analyzing in detail how each component works.

7 Drone Wars UK, "Mapping Drone Proliferation: UAVs in 76 Countries," *Global Research*, September 18, 2012, http://www.globalresearch.ca/mapping-drone-proliferation-uavs-in-76-countries/5305191.

8 William Troop, "Got Drones? The Problem with UAV Proliferation," *The World*, March 26, 2012, http://www.theworld.org/2012/03/drones-proliferation/.

9 Dave Marcus and Ryan Sherstobitoff, "Dissecting Operation High Roller," *McAfee & Guardian Analytics*, 2012, http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf.

10 Martin C. Libicki, *Cyber Deterrence and Cyberwar*, Rand Corporation, Project Air Force No. 3 (2009), http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

11 Dorothy E. Denning, "Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla (Santa Monica: Rand Corporation, 2001), p. 240, http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf.

12 Ian Trainor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *Guardian*, May 17, 2007.

13 Even and Siman-Tov, *Cyber Warfare*.

14 In this incident, malicious code was inserted on August 15, 2012 into the computer system of Aramco, the government-owned Saudi oil company. According to reports, some 30,000 computers were damaged.

15 Isaac Ben-Israel and Lior Tabensky, "An Interdisciplinary Look at Security Challenges in the Information Age," *Military and Strategic Affairs* 3, no. 3 (2011): 21-37, www.inss.org.il/upload/(FILE)1333532835.pdf.

16 Yoram Schweitzer, Gabi Siboni, and Einav Yogev, "Cyberspace and Terrorist Organizations," *Military and Strategic Affairs* 3, no. 3 (2011): 39-47, http://cdn.www.inss.org.il.reblazecdn.net/upload/%28FILE%291333532806.pdf.

17 James A. Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare," *UNIDIR Resources*, 2001, www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.

18 Rami Efrati and Lior Yafe, "The Challenges and Opportunities of National Cyber Defense," *Israel Defense*, August 11, 2012, http://www.israeldefense.com/?CategoryID=512&ArticleID=1557.

19 For instance, attacks against civilian targets, including critical national infrastructures, companies that are links in a chain of access to those targets, and companies on which an attack serves an economic need.
20 Eli Senior, "Interpol: 1,000 Cyber Attacks per Minute in Israel," *Ynet*, May 8, 2012, http://www.ynet.co.il/articles/0,7340,L-4226242,00.html.
21 Ibid.
22 See Marcus and Sherstobitoff, "Dissecting Operation High Roller."
23 Greg Farrell and Michael A. Riley, "Hackers Take $1 Billion a Year as Banks Blame Their Clients," *Bloomberg*, August 5, 2011, http://www.bloomberg.com/news/2011-08-04/hackers-take-1-billion-a-year-from-company-accounts-banks-won-t-indemnify.html.
24 Dorothy E. Denning, "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism," Committee on Armed Service, US House of Representatives, May 23, 2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.
25 See Denning, "Activism, Hacktivism and Cyberterrorism," p. 269.
26 Guy Grimland et al., "Cyber Attack," *The Marker*, January 16, 2012.
27 Or Hirshauga and Nati Tucker, "Cyber Wars against Israel: 100 Million Attacks, No Significant Achievements," *The Marker*, November 22, 2012, http://technation.themarker.com/hitech/1.1871058.
28 John D. Sutter, "Anonymous Declares Cyberwar on Israel," *CNN*, November, 2012, http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/index.html?hpt=hp_c1.
29 See Even and Siman-Tov, *Cyber Warfare*, p. 19.
30 For example, Hizbollah's cyber program. See Ward Carroll, "Hezbollah's Cyber Warfare Program," *DEFENSETECH*, June 2, 2008, http://defensetech.org/2008/06/02/hezbollahs-cyber-warfare-program/.
31 Vulnerability is a characteristic of a software/hardware/protocol component that makes it possible to use the component for a purpose other than the one for which it was intended, in a way that is advantageous to the person exploiting this feature. The advantage can be obtained in one or more of the following ways: taking control of the system, disrupting the system, or obtaining information from the system.
32 Code obfuscation is a technique from the software world that takes existing computer code that is intended to carry out a certain task and changes it in such a way that its functionality is not harmed, but the result is sufficiently different from the original so that an anti-virus program will not be able to identify it as a virus. Anti-virus programs that are based on identifying signatures in the code (a signature in this context is from a section of code intended to carry out a particular action, which can be attributed to a malicious program with a high degree of probability) will find it difficult to identify as a virus the code that was successfully obfuscated because none of the signatures known to it will appear in the result of the obfuscation process.

33 Code packing is a sophisticated type of code obfuscation. In the packing process, malicious computer code undergoes a radical change in form so that it no longer looks anything like a running code, but more like an innocent text file. This method almost completely prevents the anti-virus programs from discovering the malicious code before it begins to carry out its operation (for example, during the virus's penetration of the computer, it will not be discovered). Packing code works through an innocent utility that, when it starts to run, calls the text file in which the malicious code is hiding, translates the text into run commands, and in fact, turns itself into a virus. This can be compared to a virus from the world of biology, which takes over a living cell and exploits all of the cell's mechanisms for its needs.

34 Renana Ashuah, "Kaspersky Exposes miniFlame—Malicious Code Planned for Espionage Operations," *YedaTech*, October 15, 2012, http://www.yedatech.co.il/yt/news.jhtml?value=19827.

35 For an article on Stuxnet's successors, see Steven Cherry, "Sons of Stuxnet," *IEEE Spectrum*, December 14, 2011, http://spectrum.ieee.org/podcast/telecom/security/sons-of-stuxnet.

36 On Flame, see Aleks, "The Flame: Questions and Answers," *SECURELIST*, May 28, 2012, http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers.

37 Exploits are computer codes or files intended to exploit a vulnerability in a particular system in a manner that enables the writer of the exploit to penetrate or disrupt the system under attack. An example would be a program for viewing images on a computer screen that has a particular vulnerability that allows a code to be run on the computer under attack. Such a vulnerability is likely to be exploited in the form of an image file that includes code the attacker is eager to run on the computer under attack. Of course, such an image file must not only contain the code, but must also know how to exploit the vulnerability or the weak point of the image viewing software.

38 A patch is a system update.

39 Global Research and Analysis Team, Kaspersky Labs, "MiniFlame aka SPE: Elvis and His Friends," *SECURELIST*, October 15, 2012, http://www.securelist.com/en/analysis/204792247/miniFlame_aka_SPE_Elvis_and_his_friends.

40 This market was estimated in 2011 at more than 12.5 billion dollars, with Russia's portion of the cake some 2.3 billion dollars (nearly double its absolute value the previous year). See Group-IB, "State and Trends of the Russian Digital Crime Market, 2011," http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf.

41 Frank J. Cilluffo, Sharon L. Cardash, and George C. Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strength," *Military and Strategic Affairs* 4, no. 3 (2012): 3-23, http://cdn.www.inss.org.il.reblazecdn.net/upload/%28FILE%291362315050.pdf.

42 Denis Maselnnikov and Yuri Namestinkov, "Kaspersky Security Bulletin 2012: The Overall Statistics for 2012," *SECURELIST*, December 2012, http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012.

43 The authors were present at a meeting with a figure from the security company.