Cybercrime: A National Security Issue?

Lior Tabansky

Cyberspace, an offshoot of the development of computer and digital communications technologies, has in recent decades become part and parcel of our lives. Computerization is invaluable in improving and streamlining processes related to work, learning, and entertainment, and it affects virtually every field of human endeavor. Once the internet became commercial in 1988, it quickly turned into a mainstay of cyberspace, offering inexpensive and immediate access to many sources of information, information sharing, joint long distance work, and more.

The implications of cyberspace crime for national security derive from the way technology is used by hostile elements. This article proposes a policy directed examination of the meaning of cyberspace crime and its impact on national security, without focusing on the widespread monetary assessments of the damage caused by cybercrime. It includes a profile of cooperation among criminals, organized crime, and hostile organizations, and discusses the commercialization of cyber reconnaissance and cyber attack capabilities, made possible by ever-developing technologies and the growth of a black market in IT services. Currently, cybercrime is hardly significant beyond the realms of IT risk management and law enforcement. However, this article identifies two separate conditions where cybercrime could become a substantial threat to national security.

Public demand for cyber security rises in proportion to the growing recognition of the menace. Even in the absence of an objective increase in the scope of crime, this demand is not expected to decrease. The state's responsibility to provide security to its citizens cannot stop at the threshold

Lior Tabansky, a former Neubauer research fellow at INSS, is a doctoral student in the Department of Political Science at Tel Aviv University.

of cyberspace, and in this realm too the practical expressions of such responsibility must be defined as part of a democratic political process on a firm factual basis.

The Cybercrime Phenomenon

Computerization allows tasks to be broken down into small units and decentralizes processing; networking allows global access to information and focus on knowledge as a valuable product. Computerized technologies are implemented to change and enhance the efficiency of creative and working processes in every aspect of life, and the world of crime is no exception. The proposed definition of cybercrime is: "The use of cyberspace for illegal ends, while exploiting unique cyberspace features, such as speed and immediacy; remote operation; encryption and obfuscation, making it difficult to identify the operation and the operator."

The debate on cybercrime continues. Over a decade ago, Grabovsky wondered what was new about cybercrime, whether it was not merely an old phenomenon making use of new tools.[1] But most researchers try to analyze cybercrime as a unique phenomenon. Majid Yar categorizes it according to the object targeted: property, people, or the state.[2] Shinder and Cross distinguish between types of crime according to the level of violence involved: violent and potentially violent crime, non-violent crime (drug trade, money laundering), and crime (still) perceived to fall within the white collar category (computer break-ins, theft, and fraud).[3] According to Wall, cybercrime is "the transformation of criminal or harmful behaviour by networked technology,"[4] i.e., it developed as a result of the evolution of computerization and cyberspace and consequent new opportunities to attain, disrupt, or manipulate information for gain. Wall further classifies cybercrime into three categories: crime involving the integrity and good working order of computer systems (hacking); crime making use of cyberspace (encrypted communications among criminals, the sale of counterfeit pharmaceuticals); and crime involving computerized information contents (theft of secrets, dissemination of harmful contents).

Table 1 categorizes crime on the basis of the role played by the computer in the commission of the crime,[5] a position similar to that adopted by the European Convention on Cybercrime.[6]

Table 1. The Computer in Cybercrime

The computer as a tool in the commission of crime

Access to and dissemination of contents	Malicious disruption or modification of data	Use of communications
· Secrets · Knowledge/data · Harmful contents	· Identity theft · Fraud · Sabotage	· Harassment · Trade in forbidden materials · Spam

The computer as a target of crime

Unauthorized access	Inserting malicious code	Disruption of operation	Theft of service
· Hacking	· Malware, spyware, viruses	· Distributed denial of service (DDoS)	· Unauthorized use

There is nothing unique or new in much of cybercrime – harassment, fraud, unlawful propaganda, pornography, theft, money laundering, espionage, and so on – except the use of cyberspace. But there is another level of crime that could not exist without cyberspace: spam, click fraud, various types of malware, networks of captive computers (botnets),[7] digital identity theft, camouflage and encryption[8] of data and communications, computerized breaches of highly valuable secure facilities, and automatic, long term espionage in secure organizations, depriving them of control of intellectual property. Cyber criminals are exploiting the increasing value of digital data in all its forms, and the legal and judicial ways in which different countries handle cyberspace.

Crime has always been a widespread social phenomenon. Criminological explanations combine motivation, opportunity, and the existence of a "guarding" factor. Two different sources of human motivation can be identified.[9] Many motives for criminal behavior are intrinsic and are not determined through a cost benefit analysis. There is no reason to believe that greater use of one technology or another would change human behavior. It is therefore not surprising that people also use cyberspace to realize their needs and pursue their goals in legitimate activities – study, entertainment, education, work – as well as in the age-old human pursuits of warfare and crime.

The classic doctrine of criminology is based on the concept of free choice and a rational assessment of anticipated gain versus the risk of punishment; accordingly, the motivation for committing a crime is a rational economic decision.[10] Economists and psychologists analyze human behavior, including criminal behavior, as a derivative of a rational cost-benefit analysis. The ever-changing array of external circumstances may encourage cybercrime; this happens when someone identifies a growth in potential gain and estimates the cost – the risk of punishment – as being lower than that gain. The combination of greater digital connectivity in its current insecure form, and the increased value of computerized data results in a situation in which extrinsic motivation for criminal behavior rises.

Although developed nations have instituted regulated law enforcement mechanisms, state responses have not kept up with the pace of technological changes in cyberspace. A good example is the "traditional" bank heist as compared to cyber theft. In a traditional bank robbery security arrangements must be subdued as the chance of a confrontation with armed guards is likely. Even if the robbery itself is successful, the authorities will pursue the robbers for years to come. As cyberspace has developed, the exploitation of its vulnerability has also come to encompass bank robbery. For example, the use of botnets comprising tens of thousands of personal computers[11] for extended theft of identification details to banking sites, which are then used to steal small amounts of money, is quite common. Given the attribution problem in cyberspace, the chances of identifying the criminal are slim.[12] Financial institutions are well aware of the risk to their business interests and, together with regulatory bodies, are taking steps to protect themselves, investing in IT security to minimize the scope of opportunity available to cybercriminals. But even so, the immediate physical risk is still substantially lower for the cyber thief than it is for the "traditional" thief. The risk of legal punishment is lower as well, since cyber fraud is generally perceived by the judicial system as a non-violent "white collar" offense and treated accordingly.

The Scope of Cybercrime and Subsequent Damage: Problematic Assessments

The cybercrime phenomenon is usually examined from a variety of perspectives: legal (legislation and penalties), criminological (motivation and organization), economic (incentives and value), or technical (data

security). Jurists deal with setting the limits of what constitutes acceptable behavior and legal issues of prevention and enforcement. Criminologists apply their professional knowledge to understanding new phenomena. Economists describe the set of incentives affecting decision making by rational players. And data security experts deal with the technical aspects of technological infrastructures – software, hardware, and communications – while focusing on various vulnerabilities and ways to protect them. One thing that jurists, economists, and data security experts all agree on is that the scope and impact of cybercrime are constantly and rapidly on the rise. This assessment is based on the fact that the scope of digital data is increasing exponentially, as is connectivity between computerized facilities. Cyberspace contains more information with more potential access points for unauthorized breaches. The ordinary conclusion is that every breach exposes a growing scope of data.

Financial estimates of the scope of damage resulting from cybercrime have been issued since the 1990s, with security companies spearheading research into the subject and publishing numerous reports. There are dozens of different assessments emanating from the commercial and government sectors in the United States, England, and other developed nations.[13] An FBI report estimated damage to American business in 2005 at $65 billion.[14] In 2009, US Secretary of Commerce Gary Locke claimed that annual damage to American companies as a result of counterfeiting and piracy (i.e., illegal use of computer codes) was in the neighborhood of $200-250 billion.[15] A 2011 British report put damage at 27 billion pounds annually: the damage per annum to British citizens was estimated at 3.1 billion pounds, to the business sector at 21 billion pounds, and to the government at 2.2 billion pounds.[16] A recent report by Symantec, a leading global computer security software provider, estimated the direct damage caused by cybercrime at $114 billion annually in 24 nations.[17] Other estimates speak of hundreds of billions of dollars annually.[18]

These astronomical sums have raised question marks and doubts, but to date the impact of the criticism has been limited. Recently, two researchers at Microsoft published a position paper criticizing the shaky statistical infrastructure underlying assessments of cybercrime damage, which is typically estimated by surveys.[19] How have these estimates actually been carried out? An examination of research methods reveals how easy it is to produce inflated damage assessments. First of all, there is no information

about the use made (or not made) of data that was accessed. Those incidents where firm knowledge exists are few, whereas the scope of potential damage is huge. Let us assume that a PC storing a database of one thousand entries is breached; let us also assume that the database is not encrypted and the entries are written in plain text. Every entry represents a valid credit card, including all the information needed to use it: the number, CVC code,[20] expiry date, full name, ID number, and address of the cardholder, as well as the card issuer's bank information. In this scenario the thief sees a complete and real picture of the information on file. Yet even under these optimal circumstances, are we able to fully estimate the financial value of the information accessed? Can the thief properly assess the true value of the stolen information? Can the victim do so?

When it comes to the theft of intellectual property − the product of long research and development efforts − the victim tends to identify as damage the maximum profit he would have liked to make on completion of the R&D, manufacturing, and marketing process. Surveys, which are an appropriate method for clarifying hard-to-observe phenomena, are the main method of learning about the scope of damage. Surveys allow researchers to reach a larger, more diverse group of respondents providing their own estimates of the number of incidents and the damage, but they are also a method containing some serious drawbacks that concern social scientists and statisticians.[21] Secondly, in the absence of sufficient data, researchers use statistical methods to derive assessments from partial data.

Measurement problems affect every aspect of the debate on cyberspace threats, particularly attempts to help the discussion by quantifying damage in monetary terms. There is an inherent difficulty in estimating damage and so far it seems that monetary assessments − created by a crude use of statistical methods to present suppositions on the basis of insufficient data − are inclined to be inflated. In addition to questions of reliability of the research methods, the credibility of sources of information and the suitability of the statistical method to this type of research, there is also another problem. Monetary estimates often include indirect components of damage: whether to the reputation of the victimized organization, negative impact on consumer behavior with macro-economic implications, issues of torts, insurance, attendant expenses, or others.

Some questions central to understanding the phenomenon remain unanswered. Does it make sense to assess damage on the basis of use

actually made of the stolen information rather than maximum potential use? Perhaps it makes sense to relate to the monetary value of creating information instead of assessing its market value, present or future? And what about the cost of security and a return to normal functioning? The picture obtained from the usual sources is less than credible and the damage of inflated assessments is liable to result in a counter response of failing to take the power of cybercrime seriously enough. Basing the cybercrime debate on estimates of monetary damage detracts from a rational, intelligent, and informed debate on the problem and the ability to formulate appropriate public policy.

Cooperation between Criminals and Terrorist Organizations

The interface between professional criminals and organized crime on the one hand, and terrorist organizations on the other, is likewise not a new phenomenon. Even if we look only at the Israeli reality, we can see that such cooperation causes damage at the national level. Since 1996, the media campaign over pirated CDs has claimed that profits are used to fund Palestinian terrorism,[22] as part of a close connection between money laundering and its consumers such as terrorist organizations.[23] The widespread phenomenon of auto theft from Israel by West Bank thieves has been a feature of life in Israel for many years: the problem has hardly been confronted at national level because the threat was never considered to be a national security issue; the damage was covered by the insurance companies, which rolled it over onto the insured parties; the police took no action outside of sovereign Israeli territory; and the army – operating permanent security checkpoints on major roads – preferred to avoid dealing with a criminal population whose motivation was merely monetary, rather than nationalistic. During the "suicide bombers intifada" years the modus operandi of these criminals changed: terrorist organizations recruited the expertise of Palestinian car thieves in order to obtain cars with Israeli license plates to reach their destinations, and also to find routes to evade security checks and deliver explosives and suicide bombers into the heart of Israel's cities.

The possibilities of crossing over the fenced Gaza Strip border were more limited than between the West Bank and Israel. Tunnels were dug towards the Rafiah Egyptian border crossing to provide various kinds of smuggling channels. Smuggling generates large profits for the tunnels

operators and this activity persists despite Israel's efforts to put a stop to it. The tunnels also became a national security problem when they were used to smuggle weapons from the Sinai Peninsula to the Gaza Strip and terrorists from the Gaza Strip to Sinai.[24] It was the criminal organizations' expertise in digging tunnels that made the June 25, 2006 attack on Kerem Shalom possible, in which two soldiers were killed and a third was taken hostage by Hamas. This was a clear case of criminal technical know-how used to damage Israel's national security.

Some Bedouins in Sinai make a living from their expertise as guides and scouts, and have for decades provided smuggling services into Israel. The "goods" smuggled included, in the not too distant past, hundreds of East European women for the sex industry, as well as drugs. In recent years, tens of thousands of African migrant workers and some refugees have been guided to the Israeli border. Some believed these cases posed significant challenges but were not a national security issue. However, as the smugglers' expertise is increasingly applied to enable terrorist attacks on Israel, that assessment is changing.[25] The smuggling of terrorists from the Gaza Strip through Sinai to Israel made the August 18, 2011 attack on Route 12 possible, resulting in the killing of eight Israelis and the wounding of four. Smuggling terrorists and weapons has placed Eilat within rocket range.[26] Hence smuggling grew to become a clear and present danger to Israel's national security.

A Reexamination of the Meaning of Cybercrime

Any current examination of cybercrime reveals comparable commercial cooperation. In recent years a black market of technical experts and botnet "herders" has emerged, developing and providing technical tools and services for a price.[27] The black market of cyberspace services (Crimeware as a Service, or CaaS) causes economic damage in developed nations, though the usual monetary damage estimates are greatly exaggerated.

Anyone who prefers to operate alone and lacks R&D resources finds cyberspace weapons (toolkits of malicious software)[28] available for downloading from the internet, usually for payment of anywhere from tens to several thousands of dollars. Knowledge is an inexhaustible product, a "non-rival good" for economists, so sharing the capabilities that were available with others to you does not diminish your own strength.[29] As a result, we see a situation in which powerful tools are available to anyone

at marginal cost. The widespread impression that cyberspace makes it easier to rake in huge profits from criminal enterprises has not been lost on organized crime.[30]

Growth in computing power and the ubiquitous internet have created a new tool for extensive cybercrime: the botnet. This is a collection of internet-connected PCs whose defenses have been breached by malware and control ceded to a malicious third party, who is able to remotely control and exploit these computers on demand, usually without disrupting their normal functioning. Cybercriminals usually infect internet-connected computers with malware by exploiting known vulnerabilities that users and system administrators have failed to deal with. In 2007, McAfee estimated that some 5 percent of all internet-connected personal computers were botnet captives.[31] Large scale supply makes the cost of using a botnet affordable to virtually anyone.[32]

A newer phenomenon is the advanced persistent threat (APT), also known as adaptive persistent attack (APA)[33] – a complex, multi-stage use of cyberspace weapons for the purpose of ongoing clandestine attacks. The attacker does not operate statistically on a broad scale to exploit known vulnerabilities; instead the objective is well defined. The attacker uses a range of custom made tools, often using a valuable "zero-day" (never used before) attack mechanism. Such attacks comprise several stages and can last months or even years. The attacker begins to gather intelligence about the organizational structure of the target, and identifies people holding senior positions with access permissions for sensitive information. The gathering of personal information is usually accomplished by open source intelligence (OSInt): accessing public information and shared personal information on social networks and the news media. Once the key players are identified, a concerted effort is undertaken to steal their credentials and infect their computers.

One method is spear phishing, or inserting a remote access tool (RAT) by an email from a trusted sender with relevant content, which thus manages to bypass spam filtering mechanisms by using the personal information gathered. Opening the email allows the insertion of the Trojan horse into a trusted endpoint inside the organization's corporate network, thus gaining access to more internal resources. In a common crime, once access is accomplished, the average attacker moves quickly to retrieve valuable information and use it.

However, this is not the case with an APA attack: here the purpose is clandestine long term access, ignoring immediate monetary temptations. The attack lasts a long time, in part to overcome defense systems designed to prevent information leaks. In the course of the attack, attackers perform tests to identify the system's response thresholds and usually adapt the exfiltration methods of the stolen information. The data is divided into small packages, camouflaged inside legitimate communications, and thus leaks through the system without triggering defenses. An APA is much rarer than statistical attacks because it is much more expensive, requiring systematic intelligence gathering, planning, and adapting capabilities and the patience to carry out a long term task. Correspondingly, the damage of an APA is of a different scale.[34]

From the economic perspective, in terms of supply, hacker groups that have succeeded in developing and using software tools to control tens of thousands of computers have in fact created a service of economic value. In terms of demand, various customers − other hackers, private investigators, criminals, espionage organizations, and transnational criminal organizations − have found various uses for the product. This has created the "Crimeware as a Service" (CaaS) model, the black market counterpart to "Software as a Service" (SaaS) which has served the IT industry since 2001.[35] Over the years the model has undergone several transformations; the current buzzword for it is "cloud computing." The economic justification of the model is clear: from now on, the customer no longer needs to buy computer equipment in order to use computer services; he can simply buy the specific service he needs from large operators and use it over standard communications. The scope of the global market for this type of computer service was estimated at $14.5 billion in 2012.[36]

Let us examine the black market phenomenon from the national security perspective. The existence of a black market of cyber weapons, outsourcing research and development, quality assurance services, and technical support means that the requisite level of technical skills to become a cyber criminal has dropped. No longer is it necessary to have the competence to develop tools and methods for breaching computers oneself. The technological infrastructure needed to breach and make unauthorized use of computers is the same, regardless of whether the breach is aimed at profit, sabotage, terrorism, or destruction.[37] This reveals another risk: the use of existing tools for terrorist activity and damaging

critical infrastructures – rather than the expected fraud targets for theft and quick profits – threatens to damage national security. The continuing development of cybercrime mechanisms is therefore becoming a natural security problem.

Critical infrastructures protection (CIP) is the most important issue in cyberspace security, and the black market in cyber weapons makes the need for it even more acute. This commercialization of technical and operational capabilities allows access for many factors – including small terrorist organizations and even isolated individuals – to powerful resources with potential cyber attack application. The reference group of threats is therefore expanding beyond states and known terrorist organizations to include any element capable of purchasing commercial services available on *DarkMarket*. Nonetheless, when there is ongoing state-sponsored investment in R&D, the technological capabilities openly available on the market naturally lag behind those being developed by the security forces and a nation's institutions of higher education. Therefore the capabilities available on the market will be inferior to those accessible to state-sponsored organizations with independent R&D means, enjoying state backing in terms of resources and organization.

Towards Realizing the State's Responsibility for Cyber Security

The meaning of the cybercrime phenomenon needs to be clarified for researchers and policymakers. For the reasons stated above, monetary damage assessments do not provide a firm factual basis for understanding the concept or formulating policy. Therefore, a reassessment of cybercrime is required to design appropriate national policy.

Even in the absence of agreement on the scope of direct and indirect damage caused by cybercrime, it certainly affects how citizens, organizations, and society as a whole function. Citizens and small businesses are variously damaged by cybercrime. Spam, internet fraud, digital identity theft, invasion of privacy, blackmail, economic espionage, and damage to intellectual property all are widespread and harm some citizens and organizations. Although monetary assessments seem to be exaggerated, the development of cyberspace increases numbers of potential victims and expands even further ways of committing crimes against citizens and groups. Given rising awareness of the problem and the actual increase in cybercrime, citizens of developed countries will

reasonably demand the state take steps to provide personal, communal, and national cyber security. Growing media exposure of data breaches and cyber attacks is indicative of a proportionate growth of interest in the risks posed by cybercrime.

The state is fundamentally responsible for law and order and for the safety of its citizens, and is required to act to minimize damage to them. Policy should develop on the basis of understanding the broad implications of the phenomenon and a rational, informed public debate. Below are some pointers for developing such a debate.

The majority of the common phenomena classified as cybercrime have nothing to do with national security. What, then, is the significance of spreading hatred and incitement against Jews or the State of Israel while defacing Israeli websites, disseminating propaganda by means of social media and spam, hijacking social networks accounts, and creating internet videos and campaigns offensive to the public? Citizens will be vulnerable in cyberspace and the dignity of the nation and many of its citizens will be subjected to slander and defamation. However, experience shows that the public is not easily shaken by such acts. Beyond the professional realm of public relations, the damage at the national level is negligible.

What is the significance of common fraud – digital identity theft and unauthorized use of means of payment information aimed at stealing from citizens? When a citizen becomes a crime victim, the state authorities are expected and required to address the crime and deal with it. The state authorities have a range of methods to this end and the meaning of the events needs to be clarified so as to determine the appropriate policy. But from the perspective of national security, it is hard to see damage at national level as long as the rate of cybercrime is relatively low, even if it is higher than the more conventional crime rate. If, however, cybercrime grows to become a lasting and widespread phenomenon, citizens might lose their faith in state authorities that seem unequal to providing a safe and secure environment.

The current situation in developed nations is far from satisfactory. If "obedience in exchange for protection" is the condensed version of the social contract between citizens and the sovereign, then in the cybercrime area the state is defaulting on its side of the contract. Response to the new challenges requires, first and foremost, a clear understanding of the different phenomena and their implications and ramifications. Response

processes and the formulation and enforcement of policy require updated regulation and legislation. Legislation, which by definition lags behind technological developments, lies within the sole purview of the state. The sovereign enforcement bodies operating on the basis of national legal infrastructures will have to allocate more resources to the prevention, investigation, and punishment of cybercrime. Despite the international nature of cyberspace, the state is the sole source of responsibility for the personal security of its citizens. International treaties such as the European Council's Budapest Convention on Cybercrime[38] and initiatives being developed in the UN,[39] the OECD,[40] the EU,[41] and the International Telecom Union[42] are all boosting cooperation among sovereign authorities. International cooperation may contribute to arming sovereign authorities in the fight against cybercrime, but international treaties cannot substitute for independent sovereign policy.

First, cooperation among nations in the anarchic international arena is possible only to a very limited extent and only on the basis of common interests. It may be that developed democracies will be able to formulate arrangements among themselves, but the gap between them and authoritarian regimes in terms of defining the threat seems too great. The American debate on the issue focuses on ongoing industrial espionage of intellectual property, the product of R&D in the commercial and government sectors in the United States. Over the years, senior personnel in the business and government community have become increasingly concerned about the loss of America's global economic and strategic advantage as the leading scientific-technological innovator and superpower. In fact, "loss" is not the right word, because the knowledge is not actually lost, but rather stolen through systematic, well-organized and widespread state-sponsored theft, and the culprit is China, a nation determined to catapult its economic and military might forward by copying the secrets of American research.[43] Hence discussion of the issue clearly shifts from focusing on the economy, data security, and the law, to an almost combative security dialogue.[44] For its part, China rejects these allegations outright and is worried about undermining the foundations of its regime by use of the West's internet in the name of freedom of expression.

Second, the authority and sovereignty of a state within its borders allows that state to promote independent policy: legislation and law enforcement are not dependent on international arrangements. In Israel, an

incident known as the "Saudi hacker affair" demonstrates how the debate spills over from data security into national security. In early January 2012, someone calling himself OxOmar published a list containing the personal information and credit card numbers of thousands of Israeli citizens.[45] The information published was overwhelmingly outdated, and out of 380,000 entries only a few thousand were valid. The direct damage to cardholders was zero: the credit companies cancelled the cards and issued new ones, and in any case the law obliges them to cover unauthorized use. The scope of the information revealed was also not exceptional: every day, millions of such entries are stolen on the internet. The details are bundled according to different parameters and sold as dumps[46] to black market customers, as described above.

It soon became clear this was a simple attack: spyware had been inserted into a number of commercial Israeli websites, which transferred data stored by the site operators with gross disregard for data security. Although the attack lacked complexity and no real damage was incurred by the Israeli citizenry, the extensive media coverage of it lasted some three weeks and was initially tinged with panic and hysteria. The event was presented as anti-Israeli terrorism, because instead of realizing monetary profits from the information, the attacker chose to use it to propagate fear in the target country.

This event can be analyzed in any number of different ways. One may claim that citizens are unaware of data security; that the media are irresponsible and blow a marginal event out of all proportion, sowing panic; that website owners were careless or even criminally negligent in failing to secure the data in their possession; that the state neglected to create a safe environment for internet commerce and secure personal data. But in any analysis, the inevitable conclusion is that the personal and collective security of Israel's citizens in cyberspace needs to be upgraded. At the end of the day, that demand is directed at the state, which is responsible for its citizens' security and safety.

It is possible, even desirable, to discuss the definition of unwanted and criminal phenomena in cyberspace, the proper level of security, the division of responsibility, heightened user awareness, the limits of state involvement, and other dilemmas relevant to the matter. In a democracy, such issues are clarified through public discourse and political process. It cannot be assumed that the demand for cyberspace security will disappear,

that the problem will go away, or that the state will be able to shrug off its responsibility towards citizens. In the aforementioned Israeli case, nothing exempts the state authorities from responding to various citizen demands and undertaking legal and regulatory changes to increase data security on commercial websites. Failure to regulate and enforce law and order in cyberspace will enable a range of cybercrime to flourish, to the point of real threats to national security: providing service to hostile elements aiming to carry out cyber attacks and increasing the scope of crime to the point of compromising both personal security and the nation's business environment.

A Dangerous Interface: Cybercrime as a National Security Threat

Cybercrime continues to grow and challenges developed nations in different ways. Existing information about cybercrime is acquired from periodic reports by consulting, IT and information security companies, and law enforcement agencies. Given the problems inherent in identifying the phenomenon, the crude use of statistical methods for a quantitative analysis, and the inclusion of indirect damage in monetary assessments, it is apparent that existing information is not reliable. It seems that monetary assessments are consistently inflated. Nonetheless, that there is great potential danger in cybercrime cannot be overlooked.

The analysis in this article shows that in effect a large range of cybercrime does not represent a threat to national security. Phenomena such as theft and industrial espionage, fraud, harmful contents, hate crime, destruction of websites, denial of service, and so on are liable to become a national security problem only if there is a marked increase in their incidence and their effects are lasting. Therefore, now is the time to take action to reduce the risk and make it more difficult for cybercriminals to operate in this realm.

Past experience shows that hostile elements recruit criminal expertise to achieve operational goals. Because of the pace of technological developments, what today are advanced IT capabilities will within very few years become inexpensive, off-the-shelf commodities. The black market of computer services makes advanced capabilities readily accessible. The evidence exacerbates the concern that in cyberspace too, cooperation among criminal elements and hostile entities exists and is on the increase.

On the basis of this analysis, focus on two major interfaces between cybercrime and national security is recommended. First, the nation state is the entity responsible for the personal and collective safety and security of its citizens. Cybercrime causes various kinds of damage to citizens and organizations. The scope of such damage is unclear and the various damage estimates proffered in the debate are largely unreliable and exaggerated. But even without agreement on the scope and damage incurred by citizens, organizations, and states, the state must still respond to the opportunities and challenges of the reality as it unfolds. With the ongoing entry of cyberspace into every walk of life, it is safe to assume that demands on the state to assure personal and national security in cyberspace will also grow. Despite the global nature of cyberspace, the state will be forced to expand its involvement considerably. The outline of state involvement in cyberspace has been emerging in recent years, one of the more loaded issues being the mutually contradictory values of privacy and national security. In a democracy, the process for formulating a government policy on cybercrime involves public debate, political battles, and long term legal treatment.

Second, the commercialization of technical and operational capabilities is lowering the threshold for entering the cyber warfare arena, expanding the reference threats beyond states and large terrorist organizations, and placing a very heavy burden on national security authorities. Cyber criminal organizations offer resources, infrastructures, and even customer service at reasonable cost. This is a market that can be exploited not only to commit crime for financial profit but also to carry out direct attacks on national security. Defending critical infrastructures against cyberspace threats is a key issue in cyber security and its importance is even greater given the prevalence of potential elements of risk capable of acquiring cyberspace weapons and recruiting "fighters" on the cyber criminal black market.

Given the analysis of the phenomenon's significance and the identification of dangerous interfaces between cybercrime and national security presented herein, the immediate state focus should be on dealing with the threat in order to prevent it becoming more acute. The state must upgrade its involvement in creating cyberspace security, but it cannot solve the problem alone. The successful realization of state responsibility for cyberspace security necessitates the cooperation of all interested parties

in the business, academic, public, and security sectors, so as to provide national and personal cyberspace security to the state and its citizens.

Notes

1 P. N. Grabosky, "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies,* 10, no. 2 (2001): 243-49.
2 Majid Yar, *Cybercrime and Society: Crime and Punishment in the Information Age* (London: SAGE Publications, 2006).
3 D. L. Shinder and M. Cross, *Scene of the Cybercrime* (Burlington, MA: Syngress, 2008).
4 David S. Wall, *Cybercrimes: The Transformation of Crime in the Information Age* (Cambridge: Polity, 2007), p. 10.
5 A. Alkaabi, G. M. Mohay, A. J. McCullagh, and A. N. Chantler, "Dealing with the Problem of Cybercrime," Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime, October 4–6, 2010, Abu Dhabi, http://eprints.qut.edu.au/38894/1/c38894.pdf.
6 CoE, "Convention on Cybercrime," Budapest, 2001, http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.
7 A botnet is a collection of internet-connected computers whose defenses have been breached and control ceded to a malicious party gaining distance control and using these computers' capabilities. A botnet is commonly used for sending spam, attacking DDoS, and continuous data theft. See https://www.checkpoint.com/products/anti-bot-software-blade/anti-bot-software-blade-landing-page.html.
8 Asymmetric key cryptography is the basis of the RSA algorithm developed by Leonard Adelman, Adi Shamir, and Ron Rivest, and presented publicly in 1978. Its patent expired in 2000. PGP (Pretty Good Privacy) developed by Phil Zimmermann in 1991 was the first software to allow free use of strong encryption using this method . The common web security standards (HTTPS, TLS/SSL, SSH, Bitcoin) are employing the same public key cryptography principle.
9 Richard M. Ryan and Edward L. Deci, "Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions," *Contemporary Educational Psychology* 25, no. 1 (2000): 54-67.
10 A. R. Piquero and Stephen G. Tibbetts, eds., *Rational Choice and Criminal Behavior: Recent Research and Future Challenges* (New York: Routledge, 2002).
11 The number of infected computers is itself no indication of the network's power or potential damages. See Daniel Plohmann, Elmar Gerhards-Padilla, Felix Leder, *Botnets: 10 Tough Questions* (ENISA, 2011).
12 Wall, *Cybercrime,* p. 221.
13 See for example the GAO-07-705-Cybercrime Report, June 17, 2007, pp. 16-17, http://www.gao.gov/assets/270/262608.pdf.

14 "2005 FBI Computer Crime Survey," p.10, www.fbi.gov/publications/ccs2005.pdf.

15 Melissa E. Hathaway, "Falling Prey to Cybercrime: Implications for Business and the Economy," ch. 6, in *Securing Cyberspace: A New Domain for National Security* (Queenstown: Aspen Institute, February 2012).

16 Office of Cyber Security & Information Assurance in the UK Cabinet Office and BAE Detica,: "The Cost of Cyber Crime," 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf.

17 "Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually," http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02.

18 M. Lesk, "Cybersecurity and Economics," *IEEE Security & Privacy,* 9, no. 6 (2011), p. 76; Carl Bialik, "A Cybercrime Stat's Nine Lives," *Wall Street Journal,* September 26, 2007, http://blogs.wsj.com/numbersguy/a-cybercrime-stats-nine-lives-194/tab/print/.

19 Dinei Florêncio and Cormac Herley, "Sex, Lies and Cybercrime Surveys," Microsoft Research, 2012. The study was condensed and appeared as an op-ed piece in Dinei Florêncio and Cormac Herley, "The Cybercrime Wave That Wasn't," *New York Times*, April 15, 2012, https://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=3&hpw.

20 Card Verification Code – the secret three-digit code printed on the back of credit cards, used to verify the validity of the card details when the card is not being read magnetically.

21 This discussion exceeds the scope of the present article. For a good overview, see the chapter on surveys in Francis C. Dane, *Evaluating Research: Methodology for People Who Need to Read Research* (Los Angeles: Sage, 2011).

22 "Counterfeit CDs are Money for Islamic Terrorism," *Ynet*, January 16, 2003, http://www.ynet.co.il/articles/0,7340,L-2378873,00.html.

23 J. Hunt, "The New Frontier of Money Laundering: How Terrorist Organizations Use Cyberlaundering to Fund Their Activities, and How Governments Are Trying to Stop Them," *Information and Communications Technology Law* 20, no. 2 (2011): 133-52.

24 Israel Security Agency, "Report on Hamas' Use of Underground Passages in the Gaza Strip," November 2008, http://www.shabak.gov.il/publications/study/Pages/hamas-tunnel-report.aspx.

25 Israel Security Agency, "Smuggling Weapons to the Gaza Strip from Iran via Sudan and Sinai," http://www.shabak.gov.il/publications/study/Pages/Sudan120511.aspx?webid=a3db3c16-25d8-423d-98df-eb1b9253ab93 .

26 Meir Amit Intelligence and Terrorism Center, http://www.terrorism-info.org.il/malam_multimedia/Hebrew/heb_n/html/ipc_272.htm.

27 Nir Kshetri, "The Global Cybercrime Industry and Its Structure: Relevant Actors, Motivations, Threats, and Countermeasures," in Nir Kshetri, ed, *The*

Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives (Heidelberg; London: Springer, 2010); Misha Glenny, *Darkmarket: Cyberthieves, Cybercops, and You* (New York: Alfred A. Knopf, 2011).

28 Cyber weapons may be categorized by their intended usage: malware – malicious software meant to disrupt the normal workings of a computerized system clandestinely, thereby damaging the process controlled by that system; spyware – malicious software meant to gather data clandestinely and sometimes transfer it over the internet; scanners to identify known vulnerabilities; remote and local exploits – to exploit known vulnerabilities; network sniffers – to eavesdrop on communications; backdoor tools, Trojan horses – for distance access and data retrieval.

29 See Isaac Ben-Israel and Lior Tabansky, "An Interdisciplinary Look at Security Challenges in the Information Age," *Military and Strategic Affairs* 3, no. 3 (2011), p. 24, http://www.inss.org.il/upload/(FILE)1333532835.pdf.

30 Phil Williams, "Organized Crime and Cybercrime: Synergies, Trends and Responses," *Global Issues* 6, no. 2 (2001): 5.

31 McAfee, "Virtual Criminology Report: Organized Crime and the Internet," December 2007, www.mcafee.com/us/research/criminology_report; C. Czosseck, G. Klein, and F. Leder, "On the Arms Race around Botnets: Setting up and Taking Down Botnets," paper presented at the Cyber Conflict (ICCC), 2011 3rd International Conference, June 7-10, 2011.

32 "Kaspersky Reveals Price List for Botnet Attacks," July 23, 2009, http://www.computerweekly.com/news/1280090242/Kaspersky-reveals-price-list-for-botnet-attacks. It seems that the cost continues to drop. See Plohmann, Gerhards-Padilla, and Leder, *Botnets: 10 Tough Questions.*

33 Jeffrey Carr, November 2, 2011, http://jeffreycarr.blogspot.com/2011/11/words-matter-dump-apt-for-apa.html.

34 All high profile cases of cyber espionage, such as "Gh0st RAT," RSA/Lockheed-Martin, and "Flame" are examples of an APA.

35 *Software as a Service: Strategic Backgrounder* (Washington, D.C.: Software & Information Industry Association, February 28, 2001), http://www.siia.net/estore/pubs/SSB-01.pdf.

36 https://www.gartner.com/it/page.jsp?id=1963815.

37 Lior Tabansky, "Basic Concepts in Cyber Warfare," *Military and Strategic Affairs* 3, no. 1 (2011): 75-92, http://www.inss.org.il/upload/(FILE)1308129610.pdf.

38 CoE, "Convention on Cybercrime." Since 2001, the convention has been ratified by 30 of the 46 signatory nations.

39 T. Maurer, "Cyber Norm Emergence at the United Nations: An Analysis of the UN's Activities regarding Cybersecurity," Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

40 OECD, "Communiqué on Principles for Internet Policy-Making," June 29, 2011.

41 EU, Europol, the European Cybercrime Centre (EC3) officially commenced its activities on January 1, 2013, https://www.europol.europa.eu/ec3.

42 ITU, *National Cybersecurity Strategy Guide*, September 2011.

43 Mike McConnell, Michael Chertoff, and William Lynn, "China's Cyber Thievery is National Policy-and Must Be Challenged," *Wall Street Journal*, January 27, 2012; Richard Clarke, "How China Steals our Secrets," *New York Times,* April 2, 2012; Nathan Gardels, "Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly," *New Perspectives Quarterly* 27, no. 2 (2010):15-17; Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011); U.S.-China Economic and Security Review Commission (USCC), *2009 Report to Congress of the U.S.-China Economic and Security Review Commission.*

44 See Myriam Anna Dunn and Kristian Søby Kristensen, eds., *Securing "the Homeland": Critical Infrastructure, Risk and (In)Security* (London: Routledqe, 2007).

45 Ro'ee Goldenberg, "The Bank of Israel: Details of 15,000 Credit Cards Stolen," *Globes*, January 3, 2011, http://www.globes.co.il/serve/globes/printwindow.asp?did=1000712125; Yazan al-Saadi, "Saudi 0xOmar: Hackers of the World Unite Against Israel," *al-Akhbar English,* January 16, 2012, http://english.al-akhbar.com/node/3413.

46 Dump: a stolen credit card or bank account and the associated customer data. T. J. Holt, and E. Lampke, "Exploring Stolen Data Markets Online: Products and Market Forces," *Criminal Justice Studies* 23, no. 1 (2010).