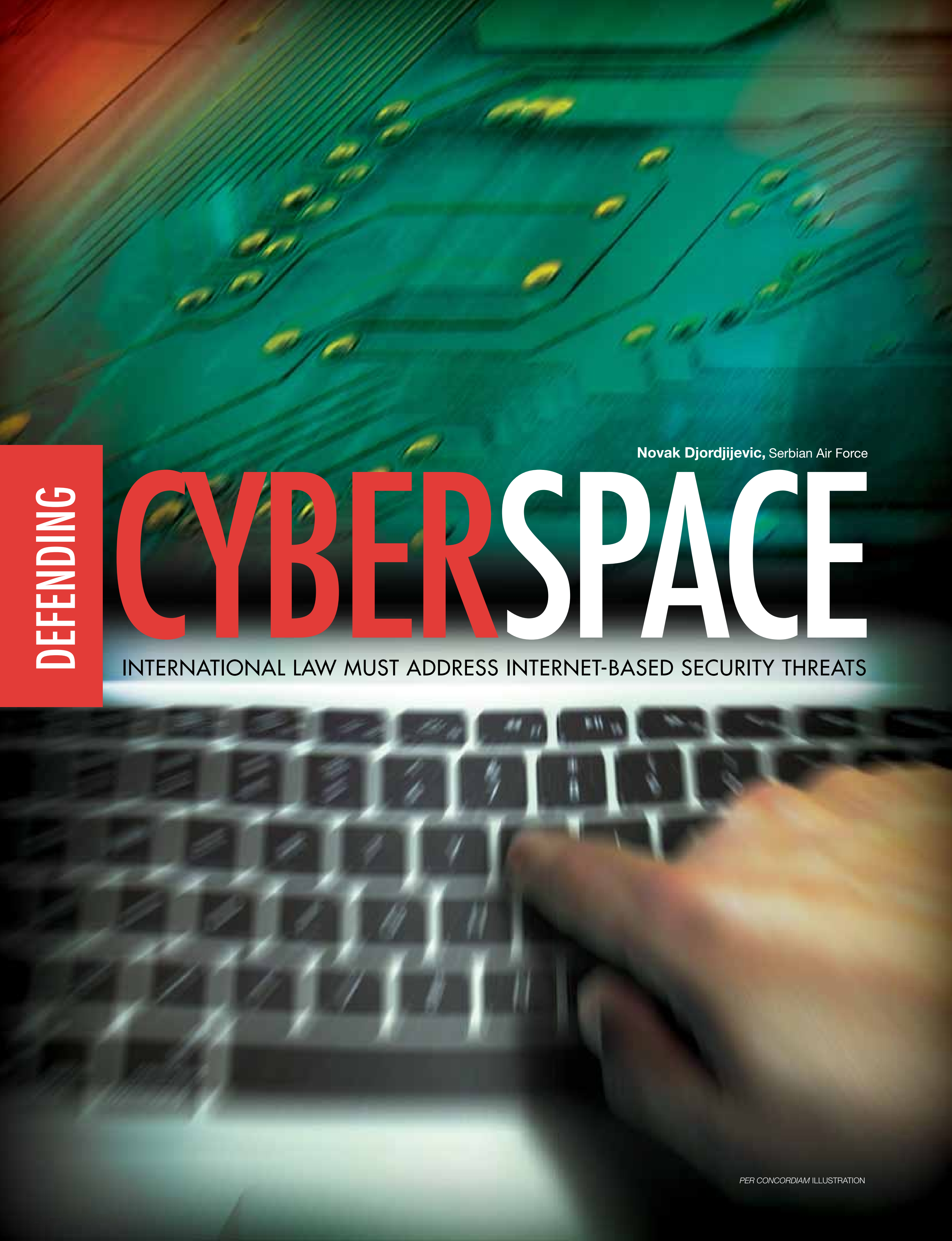
DEFENDING CYBERSPACE

INTERNATIONAL LAW MUST ADDRESS INTERNET-BASED SECURITY THREATS

Novak Djordjijevic, Serbian Air Force



PER CONCORDIAM ILLUSTRATION

Contemporary security threats are characterized by, among other things, asymmetry and flexibility. However, in the modern world, security threats transcend the limits of the physical domain, physical security and freedom of the individual and impinge on the economic, intellectual and privacy domain. In addition to activities and relationships in the physical domain of reality, using services available over the global network — the Internet — we communicate, exchange information, perform tasks, have fun and make purchases in a parallel, virtual reality. In the Internet information cloud we leave traces of our activities, traces that connect us to other people, institutions, companies and organizations. By leaving behind this information, we unintentionally reveal more about ourselves than we would have wanted.

These traces are useful information to cybercriminals. Using this and other information, cybercrime can reach unimaginable goals. In addition to individuals who are frequent points of attack, criminals are targeting websites, information portals, e-mail systems, social networks, corporate networks or networks of governmental and nongovernmental organizations, and even other criminals.

But what is a cybercrime? Simply put, cybercrime is the illegal use of computers and the Internet, or a crime committed using computers or the Internet.[1] This definition should be extended to include other telecommunication devices such as mobile phones, personal digital assistants (PDAs) and other devices that establish connections with other devices.

MOTIVATION FOR CYBERCRIME

It is often difficult to understand what drives cybercrime and motivates cybercriminals. It is difficult to classify motives, but some of the most common are listed below[2]:

- Political/religious (expansion of political, religious or other ideas, the realization of political, religious or other aims, retaliation for political or other activities, etc.)
- Financial gain
- Idealistic (activity to prove skills and abilities, without expectation of financial or other benefits or rewards)
- Curiosity, adventure (mostly beginners who have not yet entered into serious criminal activity, "coders/hackers/techies," people who are looking for a quick route to riches or fame but lack the knowledge and skill)

This limited classification helps to show how modern cybercrime is able to recruit large numbers of people. If one can promote political ideas on the Internet by illegal means, make money illicitly, or simply try to hack a site without consequences, nothing really prevents one from doing that except personal ethics. This leads to the assumption that this type of crime will continue to grow and develop. Not only has cybercrime been growing for years, but some forecast darkly[3] that production of malware (malicious software) could soon surpass production of legal software[4].

According to some experts, one of the causes for proliferating crime is an unfavorable relationship of three factors: risk, effort and benefit.[5] According to the current state of affairs, the risk that criminals face is very small and the efforts required modest, while the benefit to be achieved is relatively high. If this relationship could be reversed through use of a tailored strategy (high risk — moderate effort — small benefit), there could be a significant drop in cybercrime.

KNOW YOUR ENEMY

According to the Internet Crime Complaint Center (IC3) 2009 year report,[6] IC3 received 336,665 complaints compared to 16,883 complaints in 2000, an increase of almost 2,000 percent. The increase in financial losses in the same period is close to 3,200 percent. Most people reported financial losses in the amount of $100 to $1,000 (36.7%), and nearly 87 percent of victims lost less than $5,000. This data clearly indicates that cybercrime is growing.

However, do we take this threat seriously? The general public's understanding of cybercrime is vague. Unlike traditional forms of crime, it seems that cybercrime is faceless, and it is unclear whether the criminal structures consist of individuals, criminal groups or a combination of both. The cybercriminal personality is created because of special social, technological, economic, hereditary or other factors. Theoretically, anyone could become a cybercriminal.

The computer security firm Symantec recently published the results of a study in which it analyzed cybercrime and human relationships based on a sample of about 7,000 respondents from 14 countries.[7] Some results show that most people mistakenly believe that cybercrime is not organized crime, although the analysis revealed that "90 percent of today's cyber attacks are a direct result of organized crime." In other words, most people believe that cybercrime is an individual activity, while evidence shows that cybercrime is mostly organized crime. This means solving the problem of cybercrime requires an organized, systematic, international approach.

To determine appropriate strategies against cybercrime, it is necessary to understand the order of criminal mechanisms in the physical domain (modus operandi). This is best done through interpretation of the topology of cybercrime. Cybercriminals are often organized into small groups proficient in using software and hardware. However, criminals from a single group do not have to be in the same physical location, but can be dispersed across cities, regions, countries and even continents. In addition, they rely on hardware that can be rented in any country. Criminals can use the Internet to execute their operations remotely.

Such amorphous organizations and activities are very difficult to detect and track, and almost untouchable by legal means. This topology makes cybercrime an organized global criminal phenomenon and a growing global threat to all of us.[8] Cybercrime is like cyber cancer. The removal of one problem usually represents just a short break before a new problem pops up somewhere else. Like a cancer, cybercrime seems to elude efforts to curb it.

DEFENSE IS NOT ENOUGH

Is there a strategy for controlling the growth rate and extent of cybercrime? Why do current methods of combating cybercrime render modest results?

Methods of combating cybercrime were developed in the early days of computers, when malicious programs spread through floppy disks and the spread of a virus took a relatively long time. With the emergence of networks, dissemination of harmful programs multiplied rapidly. This means the spread of harmful programs is almost immediate. The only things that stand between two network nodes are safeguard mechanisms.

However, existing methods of protection are defensive and reactive, which means that protection systems wait for the occurrence of harmful programs (defensiveness) and recognize and block known harmful programs (reactivity), but have trouble coping with the inventiveness of cybercriminals. The reactive method means that it is possible to fight known threats. The new threat appears, after being uncovered and identified, then the appropriate protective mechanism is created (patch, infected files deletion, blockade of certain actions, etc.), and finally is distributed as part of the protective mechanism. The problem is that this process is relatively slow, so there is always damage. The security model is a shield that strives to protect the computer from attackers. Examples of access controls are firewalls, passwords, anti-virus programs and anti-spam filters. But it's just passive defense. Without active mechanisms, current security systems lack the ability to prevent the cybercriminal from causing damage before he enters the grid.

In contrast to defensive and reactive methods, active methods could be created, but it requires a significant change in the technology on which the Internet rests. First, it should be realized that cybercrime is a social activity that pervades several physical and virtual layers.

As a social individual, a cybercriminal is at the bottom of a crime scheme. This person is wrapped in layers that hide him, starting with hiding behind pseudonyms and avatars, a country's privacy laws, the characteristics of telecommunications hardware and software that may or may not track the malicious programs' network movements.

The scenario of a cybercrime occurring in one country and the criminals located in another country could be called a "crime projection," where the cause of the problem is not creating a problem in its environment but it is projecting it at a distance, in an environment that cannot effectively fight against pathogens. This is the fundamental strategy of cybercrime, which allows it to survive and develop almost undisturbed. To fight this strategy, a global response needs to be developed.

A GLOBAL RESPONSE

Good active strategy against cybercrime would imply:

- Legal regulation of international relations in terms of cybercrime treatment.
- Redefining telecommunications standards (hardware, software).
- Redefining the framework of privacy protection.
- User education (positive social engineering).
- International cooperation and coordination regarding criminal detection, monitoring and elimination.

The essential obstacle to dealing with cybercrime is the inadequacy of legal mechanisms. Laws established at the state and interstate level are the underlying premise for creation of a global mechanism for combating cybercrime.[9] Of course, the fight against cybercrime is possible even in the existing model of "every man for himself," but such a model is expensive, barely effective and hardly sustainable. In the longer term, if there is no significant change regarding cybercrime, each of us will be chasing one piranha while the piranha pack is devouring us all.

Redefined telecommunications standards would allow for information traffic flow monitoring and recording of the source, path and destination of telecommunications packages. This would enable authorities to — if necessary — analyze traffic data and identify the sources of criminal activity. This would be a key support mechanism for detecting and identifying cybercriminals.

However, it is certain that this would raise great privacy concerns. Traffic flow records would have to be stored and safeguarded for some time. It is a serious issue outside the scope of this paper, but let's mention one scenario. If someone illegally accesses traffic flow records, he could erase them or extract information, using data mining and other techniques, for illegal gain (e.g. competitive advantage). This problem requires legal regulations, access limits and appropriate software and hardware applications.

Education requires extensive and continuous effort, but it is at precisely this level that one can achieve the best and most enduring results. Proper education significantly reduces the chances that individuals become victims of cybercriminals. On the other hand, criminals have long used social engineering to persuade the individual to "click here" and become a victim. Education in this field is just as necessary as literacy education was a few centuries ago. However, in addition to education for ordinary computer users, the world needs education for professionals. That's especially true for professions that deal with cybercrime but lack technical training: judges, lawyers and prosecutors in the EU.[10]

In the absence of a more extensive and generally accepted international policy to combat cybercrime, individuals,[11] NGOs,[12] academic institutions[13] and security equipment and software manufacturers took the initiative, despite relatively diverse interests. Individuals, nonprofit organizations and academics have largely focused on the need to solve the problem systematically (public information, education, defining new security strategy, open software, etc.), whereas the interest of manufacturers lies partly in achieving higher profits.[14]

Coordinating anti-crime activities on the international level is complex. Activities of this type require participation of many actors, some of whom have begun to take matters into their own hands, not willing to waste more time waiting for governments to realize the need for international agreement on the issue.

FIRST STEP, LONG JOURNEY

The current security situation with regard to cybercrime is too lax. It's like a huge dam, patched up to avoid deterioration, that is about to collapse with negative security, political, financial and social consequences. Security mechanisms developed so far are no longer effective enough. They even generate an unwelcome side effect — the illusion of security.

In the current situation, where everyone takes care of his own problems, everyone fights cybercrime anyway he can. The state may have laws and enforcement mechanisms. Institutions may have hardware and software protection designed and maintained by professionals. An individual may have a personal protection system. The security device and software market is growing — it grows and develops to keep pace with the crime rate. Known names in the field of security earn big profits, but despite the benefits of the status quo, they recognize[15] that the challenges are growing.[16]

Cybercrime is a serious threat to all. It must be taken seriously. Simple actions limited to a single country will achieve modest results. Our semblance of security can be blown at any moment with a cybercrime on a horrific scale.

The road to creating an active protection model must cross many obstacles, one of which is the creation of international laws against this type of crime. Other problems are organizational and technical and will be easier to overcome once an international legal basis for the fight against this new global threat is established. □

[1] The Free Dictionary, http://www.thefreedictionary.com/Cybercriminal

[2] Wipul Jayawickrama, "Cyber crime – Threats, trends and challenges," Computer security week 2008 – Brisbane, http://www.auscert.org.au/download.html?f=290

[3] Symantec, "Symantec Internet Security Report, Trends for July – December 07," published in April 2008, citation: "the release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications. " http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf

[4] Dr. Igor Muttik, "Cooperation is key to Internet Security", McAfee Security journal 6/2010, citation: "If we do not succeed in stopping the malware flood, then in a few years we could see more malware created than legitimate programs."http://www.mcafee.com/us/local_content/misc/threat_center/mcafee_security_journal_summer2010_en.zip

[5] Joe Stewart, "Beyond takedowns: Offense in Depth," McAfee Security journal 6/2010 http://www.mcafee.com/us/local_content/misc/threat_center/mcafee_security_journal_summer2010_en.zip

[6] Internet Crime Complaint Center, "2009 Internet Crime Report," published in 2010, see pages 2 and 6, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf

[7] Same as footnote 1.

[8] National Fraud Center, "The growing global threat of economic and cyber crime," December 2000, http://www.utica.edu/academic/institutes/ecii/publications/media/global_threat_crime.pdf

[9] International Telecommunication Union, "ITU Toolkit for cybercrime legislation," http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html , citation: "The adoption by all countries of appropriate legislation against the misuse of ICTs for criminal or other purposes, including activities intended to affect the integrity of national critical information infrastructures, is central to achieving global cyber security."

[10] Cybexa in partnership with UNICRI (financed by European Commission (AGIS 2005)), "European Certificates on Cybercrime and Electronic Evidence," http://www.unicri.it/emerging_crimes/cybercrime/cyber_crimes/ecce.php

[11] Example: http://www.schneier.com/

[12] Example: http://www.owasp.org/index.php/Main_Page

[13] Example: http://cci.ucd.ie/

[14] Example: "The Symantec Alliance Network provides a platform for expanding their channel partner ecosystem and driving more revenue with their solutions." http://www.symantec.com/about/news/release/article.jsp?prid=20100923_01

[15] McAfee, "McAfee Virtual Criminology Report - Cybercrime: The Next Wave," citation: "Ingenious cyber criminals have evolved "super-strength" threats that are harder and harder to detect and can be modified on the fly." http://www.mcafee.com/us/research/criminology_report/default.html

[16] Safe Internet Alliance, "International cyber crime creates new challenges for US authorities," http://safeinternet.org/blog/international-cyber-crime-creates-new-challenges-us-authorities