UNODA Occasional Papers

No. 19, June 2010

CYBERWARFARE AND ITS IMPACT ON INTERNATIONAL SECURITY

19 February 2009, United Nations, New York

UNODA
United Nations Office for
Disarmament Affairs

Organized by the
United Nations Office for Disarmament Affairs

United Nations

UNODA

United Nations Office for
Disarmament Affairs

UNODA Occasional Papers

No. 19, JUNE 2010

CYBERWARFARE AND ITS IMPACT ON INTERNATIONAL SECURITY

19 February 2009, United Nations, New York

Organized by the
United Nations Office for Disarmament Affairs

United Nations

UNODA Occasional Papers is a series of ad hoc publications presenting, in edited form, papers or statements made at international meetings, symposiums, seminars or workshops organized by the Office for Disarmament Affairs or its regional centres in Lima, Lomé or Kathmandu. They deal with topical issues in the field of arms limitation, disarmament and international security and are intended primarily for those concerned with these matters in Government, civil society and in the academic community.

The views expressed in *UNODA Occasional Papers* are those of the authors and do not necessarily reflect those of the United Nations, or of their Government or institutions or organizations with which they are affiliated.

Material appearing in *UNODA Occasional Papers* may be reprinted without permission, provided the credit line reads "Reprinted from *UNODA Occasional Papers*" and specifies the number of the *Occasional Paper* concerned. Notification to the following email address would be highly appreciated: unoda-web@un.org.

This publication is also available at

www.un.org/disarmament

UNITED NATIONS PUBLICATION

Sales No. E.10.IX.4

ISBN 978-92-1-142275-7

Printed in United Nations, New York

Contents

Foreword v

Presentation

Cyberwarfare and its impact on international security
by James Andrew Lewis 3

Appendix

Members of the Advisory Board on Disarmament Matters 23

Foreword

The United Nations Secretary-General's Advisory Board on Disarmament Matters held its fifty-first and fifty-second sessions in New York from 18 to 20 February 2009 and in Geneva from 1 to 3 July 2009, respectively. As part of the improvements made in its method of work since 2008, the Board focuses its deliberations during both its annual sessions on two or three substantive agenda items.

In 2009, one of the substantive agenda items for discussion included "Cyberwarfare and its impact on international security". The Board was able to conduct a stimulating exchange of views on matters pertaining to cyberwarfare and security. With regard to the topic, the Board suggested that the Secretary-General should raise the awareness of both governments and the general public of the emerging risks and threats related to cyberwarfare whenever possible.

At its February session in New York, James Andrew Lewis, Senior Fellow and Program Director at the Center for Strategic and International Studies, provided the Board members with a presentation on the issue of cyberwarfare and security. The Office for Disarmament Affairs is grateful to James Lewis for his presentation to the Board.

UNODA is publishing this Occasional Paper *for the benefit of all those who were unable to participate, in an effort to stimulate further interest and discussions on the topic of cyberwarfare and it impact on international security.*

- Ed.

Presentation

Cyberwarfare and its impact on international security

by James Andrew Lewis[1]

Abstract

The challenges of addressing cyberwarfare and cybersecurity, which are relatively new issues, have many countries unprepared and ill-equipped. The virtual, global and anonymous nature of cyberconflict creates complex difficulties in formulating counter-attack and deterrence strategies. Other problems include the speed required to cope with such attacks, an inadequate terminology or lexicon, an outdated Internet architecture, problematic assessment of collateral damage, verification of agreements, identification of technologies involved, and the need for balance between Internet privacy and control.

I STARTED WORKING ON THIS ISSUE about 12 years ago when I was still a government employee. I was looking at the commercialization of the Internet and increasing cybersecurity. Since that time, I have written seven or eight different studies and produced one book on this issue. Most of them have looked at the security implications of the Internet.

The Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency released its final report entitled "Securing Cyberspace for the 44th Presidency" in December 2008.[2] Intended to provide strategic insights and practical

[1] James Andrew Lewis is a senior fellow at the Center for Strategic and International Studies (CSIS) and directs its Technology and Public Policy Program. He was Project Director of the CSIS Commission on Cybersecurity for the 44th Presidency.

[2] "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency", Washington, DC, December 2008. See also http://csis.org/publication/securing-cyberspace-44th-presidency.

policy solutions to the incoming Obama administration, 40,000 copies have been downloaded.

I am going to speak a little bit about the report and some of the issues that we uncovered. It was carried out by a group of about 40 experts in cybersecurity, all with government backgrounds from different agencies: the Department of Defense, the Treasury Department and agencies across the United States Government.

We looked extensively at some of the international issues. As an aside, I would mention, the previous United States Administration had something that it called the comprehensive national cybersecurity initiative. The most interesting thing about this was that it was not actually comprehensive, even though that was its name. It was not comprehensive in several ways. It looked at just securing the ".gov space"—that's the networks of the United States Government. It did not look at commercial networks and most importantly it did not look at how to work with our international partners. So this is, of course, a crucial problem. It is a global resource that we are talking about. We are all part of a single, global network. Sometimes we like to think of it in its fragmentary pieces but the best way to approach this is as a single, global network in which we all participate and share. That said, it is very difficult to think about this for a number of reasons and I wanted to walk through them.

Here are some of the problems we uncovered. First of all, when we talk about security on the Internet, we need to be more precise about what that actually means. A CSIS report from 2003 started by looking for cyberterrorism. Since we hear about cyberterrorism all the time I thought of looking for examples and write down what actually happened. What I found is that there is no cyberterrorism. There have been no terrorist incidents, attacks on critical infrastructure or casualties. One reads all these stories in newspapers about dams that were opened. I called people who worked at the dams—they never heard of it. Following up on reports of police emergency systems being shut down, I called the police departments in question and they did not have any problems. Upon further investigation of all these incidents, one finds quickly that the causes were actually not cyber-related.

Let us talk about the implications of misestimating the problem, as much of the thinking and work on this has been inaccurate. As the

CSIS Commission on Cybersecurity further looked into cybersecurity issues, it decided that the leading problems were principally crime and espionage, followed by inter-State conflict. Cyberterrorism was not considered because of the difficulty to verify its existence. Not realizing that crime and espionage are the principal problems for cybersecurity leads us to misestimate the threat.

This is information warfare. It is about intangible goods and services. It is very different from conventional warfare. Some have probably seen the Hollywood blockbuster movie, *Die Hard 4*, where hackers brought down the United States. Nothing shown in the film can really happen. We are talking about a very different kind of conflict and it is one that people are beginning to think about. People are beginning to attempt to describe it.

Allow me to provide you with another example that might be more familiar: Estonia. The Estonian Minister of Defense and some of his cybersecurity staff came to CSIS in order to exchange views. Once again, it is easy to overestimate what happened in Estonia. We had our own Secretary of Homeland Security give a speech to a huge audience in San Francisco where he announced that Estonia had been brought to its knees by a cyberattack. At that moment, I walked out of the speech because that is just completely wrong—Estonia was not brought to its knees. Some Government networks had slower services and went offline for a day or two and had to be restored. There was difficulty in using ATM machines and in making electronic banking transactions from outside of the country.

This was not a crisis, a war, nor terrorism. Yes, it was part of a larger political campaign. When I think of this incident in Estonia, I see it more as like a political disturbance where a foreign power may hire a mob to hold a rally in protest of a certain cause at the capital of another country. So this was more like a cybermob and a noisy demonstration. Furthermore, the incident did not actually disrupt critical services in Estonia, such as military and long-term economic capabilities. If these were unaffected, we have to ask: what was the benefit of the so-called cyberattack? There are interim disruptions that can occur, of course. One can think of services that can be disrupted and for me the most interesting targets were the telecommunications networks, the financial networks and the electrical grid. These are valuable targets and they should be highly defended. In the United States, two out of three of these are highly defended. If one thinks about what constitutes a cyberattack, these are intangible in many ways. Such an attack does not produce kinetic or explosive results in most cases and works best against large, aggregated, national- and international-level networks like telecommunications or finance. Therefore, it is a very different kind of war.

Espionage is worth talking about because, for the United States, this is the principal problem. The loss of intellectual property and military technology has been very damaging in the last 5 to 10 years. This has also occurred in other countries. In fact any country with good technology on a computer network is a target. Who are they a target of? I want to come back to that but let me discuss one of the implications of this situation. We are indeed talking about a very different kind of conflict.

Sometimes, when I talk to our Department of Defense, I tell them that they are in the same situation as the generals in 1913 when they looked at the airplane. It was made in a bicycle shop, constructed out of string and cloth. The best it could be, they thought, was a replacement for the horse. However, four years later, they had very different ideas of what conflict with aircraft looked like.

We are at that point where we do not yet fully know what the military implications will be for this new technology. One reason that we do not know is that we have a very imprecise lexicon for describing cyberconflict. This weakness is in the terms we use to describe things. This is linked to the misestimation problem. Many of the early scenarios which one may have read about are an electronic Pearl Harbor or buildings falling down. I have what I call a Godzilla test—if an attack is something that Godzilla, the movie monster, would do, then it is unlikely that it would ever happen because of a cyberattack. That test still works.

If one thinks about what constitutes a cyberattack, these are intangible in many ways. Such an attack does not produce kinetic or explosive results. Therefore, it is a very different kind of war.

What does it mean to have a weak lexicon? This means that it is hard to discuss this issue. In the United States, we have been discussing cybersecurity for several years, trying to refine our concepts and terminology, and it has been difficult. To be clear, when we talk about cyberconflict, it is not terrorism. Hackers do not create terror. We all know what terror looks like—this is not terrorism. It is not necessarily war either. It may be an adjunct to war. It is now part of some countries' portfolio for beginning an attack, which is a useful indicator. If one's websites are suddenly being flooded with packets, it is what we would call an indicator and warning of a potential attack. However, it is not warfare in the traditional or conventional sense. Finally, and perhaps most importantly, cyberattack does not involve weapons. This is a hard concept to deal with because, in fact, the most valuable attack unit is a person with programming skills.

The most viable attack vector is what we would call social engineering. For example, I could take a thumb drive[3] with malicious software on it and throw it out onto someone's parking lot. Being a good citizen, someone would pick it up, wonder who it belonged to, and plug it into his new computer. That would spread the virus. I could also scatter thumb drives in a restroom. Someone just did that in the Department of Justice. A bunch of thumb drives were scattered in the Department, which runs the Federal Bureau of Investigation and the whole Attorney General's office. Fortunately, whoever picked up the thumb drive was smart enough not to plug it in, as it did have malicious software on it. But how would a thumb drive be described as a weapon? One could call it a dual-use item, but it is essentially a commercial item.

Some of this is also related to the way the Internet is architected. I actually got to use the Internet when I was a child. The physics department in the school I went to had one of the 12 Internet terminals that existed in 1984. If one wanted to send an email, one could go to the physics department, type his message and then hand it to someone who would send it. He would come back three hours later and in his mailbox there would be a printout of the reply. That was the Internet. Everyone knew who was on it. They knew I was in Chicago,

[3] A USB flash drive, also called a thumb drive, is a flash memory data storage device that is typically removable and rewritable. Most flash drives use a standard type-A USB connection allowing plugging into a port on a personal computer, but drives for other interfaces also exist. See also http://en.wikipedia.org/wiki/USB_flash_drive.

I knew they were in Caltech. There were no strangers. That is the way this was designed. Unfortunately, the Internet has grown immensely beyond that. Instead of a few thousand scientists using it, there are now hundreds of millions of users.

The Internet's architecture is inadequate in two ways. First of all, the rules that govern how the Internet operates are still protocols of the 1970's and 1980's. They are ridiculously antiquated. They were designed for a community of scientists who all knew each other. They are not appropriate for a huge global network. Changing the protocols is one of the major tasks that we as a global community face. In the interim, what that means is that this is a very porous environment that provides many opportunities for attackers armed with nothing more than a laptop and some programming skills. With that, they can attack the entire world. Again, I go back and say that our lexicon is weak —when I say "attack", it conjures up images of warfare and violence. Attack is different in this new way. What they can do is penetrate networks, implant malicious codes, download information and disrupt the services provided by those networks. That is what we actually mean. That is different from a traditional attack, but it is risky and it could be damaging.

The Internet's architecture is inadequate in two ways. First of all, the rules that govern how the Internet operates are still protocols of the 1970's and 1980's. They are ridiculously antiquated. Another weakness is the problem of attribution.

Another weakness of the outdated Internet architecture is the problem of attribution. I want to focus on this and I will come back to this several times. Attribution means knowing who is the person at the other end. Some people call it authentication, while others call it identity management. Attribution is relatively new. Let's think about what diplomats did two hundred years ago. One got a letter presumably from the king or an authority figure and he presented the letter to the court as proof of his credentials. Practices today are still very much like that, as reinforced by the 1961 Vienna Convention on Diplomatic Relations.[4]

[4] The Vienna Convention on Diplomatic Relations of 1961 is an international treaty that defines a framework for diplomatic relations between independent

We do not have a similar process for the Internet. The famous cartoon that I am sure many have seen on the Internet shows a dog sitting in front of a keyboard and it says: “On the Internet no one knows you are a dog”. Weak attribution is a central problem for securing the Internet—we do not know who is at the other end. It can be politically charged.

There are reasons why anonymity is good in some circumstances. For example, if one browses the Internet, goes to a health website and looks up a disease, one may just be curious or is attempting to diagnose oneself. Currently, most of those sites might be able to collect one’s information being transmitted and from which computer he or she is contacting them, but they do not know who the person is sitting behind that computer. And so there is nothing they can do with that information. If one is firmly authenticated, owners of the sites visited might be able to sell the person’s information to an insurance company or a drug provider, or use it for some other purpose. Anonymity protects privacy and, to some extent, political speech. So there is a value to anonymity, but it also creates immense risks. On the Internet we are currently tilted so far in favour of anonymity that it is going to be very difficult to secure.

An anonymous Internet can never be secure.

One of the lines that we had in our report was that an anonymous Internet can never be secure. We were forced to take that out in the drafting because the privacy community became very upset with it. They like their anonymity. However, it complicates the problems of security. How does one know if an incident is a crime or an act of war? How does one know if it is a teenager, a foreign State or a criminal group on the other end? The short answer is that unless one is exceptionally lucky and quick, one will not know. One example from the United States experience is in one of the early hackings of the Department of Defense computer network. The Department decided

countries. It specifies the privileges of a diplomatic mission that enable diplomats to perform their function without fear of coercion or harassment by the host country. This forms the legal basis for diplomatic immunity. Its articles are considered a cornerstone of modern international relations. It has been ratified by 186 countries. See also http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=III-3&chapter=3&lang=en.

that it was a foreign country. They gathered together and began to plan a counterstrike at the cabinet level. The United States was about to go to a war because of this computer penetration of its defence networks. At that moment, the Federal Bureau of Investigation found out that the perpetrators were actually two teenagers in Modesto, California. If the Department of Defense had launched the strike, it would have been both a tragic error and totally useless. It would have had no value.

This is a central problem for security. How can an incident be determined as either an act of war or a crime? Under the United States legal structure, we default to crime, because if a cyber incident is treated as a crime, we know what to do, how to collect evidence and how to respond. If it is an act of war, we would not know what to do. Would one shoot a missile back? Would one try and fry the attacker's own computer? Would one send an annoying note? We do not know. One of the reasons we do not know is because we cannot tell and not on a timely basis. So this difference between crime and warfare is complicated.

The weakness in attribution also complicates this security issue because in some cases it may well be criminals acting at the behest of a State. One could call them mercenaries or patriots, but they should be called criminals because that is what they are. This means that one could be attacked by a criminal and it could be an act by a foreign State but it would be difficult to tell. If one traced it back, one could find an individual. It is difficult to determine where an attack comes from because one of the techniques now in use. It is called botnets (short for robotic networks). When I was approached about speaking to the Secretary-General's Advisory Board on Disarmament Matters, I was asked not to go into an extensive technological discussion, but let me explain what a botnet basically is. As I mentioned, we are on a single global network; we are all connected. Every time the computer is turned one, the user is connected to a billion people around the world. One of those billion people writes a program that searches across the Internet for computers with a vulnerability—and it could be any vulnerability. It could be through a printer or thumb drive. It searches across the Internet, finds a vulnerable computer and implants software on it that allows that remote criminal to control the computer. There is a very good chance the computer owner will not even know.

In the best possible case a consumer might notice that his computer is running a little slower and then blame Microsoft.

When one assembles these captured networks into these botnets one then has the ability to: (a) access massive computing power that only States once had; and (b) launch attacks from all over the world. As an example, people always try to hack into my organization, CSIS—I think it is funny because all of our work is unclassified and in the public domain. However, someone tried to hack into our system a couple of weeks ago. For fun, I decided to try and trace where these penetration networks were coming from. One was coming from a mid-sized optical equipment manufacturer in Germany, one from a travel agent in Puerto Rico, and one from an auto supply store in Detroit, Michigan. These people were not doing anything to attack or penetrate us; they were clueless. However, their computers had been taken over and were being used. So the botnet creates an even more complicated situation for attribution because, although one may be able to find out who was attacking, it could be the wrong person. I want to come back to this when I talk about deterrence because this is a crucial issue.

What is the environment we are operating in? It is highly commercial. It is very fluid and the technology changes rapidly. It is an environment tilted towards anonymity. It is complex. It is millions, even hundreds of millions of devices each with different systems and software all connected to each other. It is opaque. When we talk about this now in Washington, sometimes we refer to it's as "the cloud". One connects to a cloud and does not actually know what's in that cloud. One does not know where his messages are going; one does not know who is coming. Finally, it is an environment that is marked by competition and mistrust. This is something I tell people that they just have to accept. There will be competition; people will not trust each other. One of the big avenues for mistrust is the matter that some refer to as the "supply chain problem". It used to be in old days that when I bought a box and it had a name on the outside—that was a national product. There are no national products in information technology anymore. So there is dependence on unknown foreigners to supply items that may be critical to national security.

I heard this from a European country just recently, where they were determined to secure their telecommunications network. But they found out that they no longer had a national telecommunications manufacturer. They were forced to buy from one of the four or five countries that made the equipment. Looking at those countries and tracing back the components, one would find that the hardware comes from China, the software comes from Europe or the United States and the microprocessors come from Japan, Korea or California. This is a global industry. So one would be working with components that are inherently untrustworthy. One would not be able to get trust except in a very small number of circumstances by building some specific device. That is a different way to think about the problem.

There are some solutions that just will not work in this space because we have a global supply chain. That is not going to change. There are things that the United States no longer makes, for example, flat screens. We have to buy them from somewhere. We do not make memory chips in the United Sates anymore. Where do we get them? How do we know they are safe? There have been a few instances of people trying to corrupt the supply chain to get advantage. What is the advantage they get? You buy a device and it is loaded with malicious software that allows them to remotely access and control it. Frankly, I do not worry too much about supply chain attack because there are so many easier ways to penetrate a network. They would not bother. They would not infect a million Dell computers to get one person. They can do better than that with cheaper and faster means.

As I mentioned, I do not worry too much about supply chain but it is something to think about. If you have ever bought a computer, a wireless router or electronic devices, you would notice that they have default settings. The default name in usually "admin" and the default password is usually "password". Everyone on the planet knows that. So I can write a program that will search the Internet and look for machines where somebody forgot to change the defaults. Our studies show that most people do the right thing—they change the password and the username. Most people do this, but not everybody. Again, if you are talking about millions of devices and I only have to find four or five, I have an automated tool that will search the Internet and search millions of devices.

However, this question of how to secure this really complex network is a real challenge. It will take a considerable effort. I am not sure countries have even begun to focus on this now. We are still vulnerable.

How do you build trust in this kind of environment? It is anonymous, complex and opaque. It is marked by competition and mistrust. It may not be possible to greatly expand trust in this environment and so one is faced with a very difficult task. This is a long-term project that will require many steps. This is certainly how the United States is approaching this nationally. There are so many elements that complicate the situation: anonymity, which is very difficult to change; the age of the Internet protocols; the global network, but that the rules are different in each nation about what you have to do to secure things. It is indeed a challenge to get everyone moving in the same direction towards greater security, while preserving privacy and civil liberties.

There is the capability to securely identify each device, but this would involve knowing everything one did on the Internet, which of course would be unacceptable to most people. A solution must be found that balances both the need for security and political openness. This has proven to be very difficult. Without such a balance, no solution would work. If one does not address civil liberties and privacy, no solution would be permanent. This is one of the conclusions in our report.

Having said that building trust may not be possible immediately or globally, what are some things that can be done?

There was an interesting parallel with weapons of mass destruction that we discussed extensively in our report. How did the world respond to weapons of mass destruction (WMD)? When WMD was just a new security problem that the world was just beginning to face, the United States first built some national structures, such as creating offices in the White House, the State Department, the Central Intelligence Agency, the Department of Defense and even the Commerce Department to deal with non-proliferation. Laws and regulations that covered the sale of goods that could be used for proliferation purposes were established. Most importantly, we worked closely with international partners. There was a realization that one country could not address the WMD problem by itself and that it was a global problem.

The United States has not done any of that for cybersecurity. We are completely disorganized. I actually spoke to some French colleagues who came from the Prime Minister's Office two months ago and their first question was, "When we come to Washington, we do not know who to call. Who is in charge?" The answer is that, unfortunately, no one is in charge. This question can be asked in one's own country: who is in charge of cybersecurity? Not having an answer complicates things.

This makes the WMD model attractive because it gives us a road map on what we can do nationally and internationally. There is a need to think about the norms in cyberspace and against certain kinds of activities. At present, the problem is that there are no generally accepted standards. These cannot just be dictated, however, as they have to be developed organically by a group. Those present today may have taken part in the process of creating norms against proliferation of missiles or nuclear, chemical and biological weapons. Think about how long that took. Based on this model, we would be where we were in the early 1990s.

We are at a very early stage of thinking about how to address cybersecurity as a global community. One lesson that may be drawn from the WMD experience is that sometimes it is more effective to begin work with like-minded countries. In our report, we recommended that the United States administration follow two tracks.

The first is what we call the "big tent" approach, acknowledging the global network and considering cybersecurity a global problem. All share responsibility in some way, with a need for a global venue to discuss the issue, while remaining cognizant of the slow and erratic progress of such a global approach. There is a complex problem presented here.

Another approach is based on like-minded nations. Drawing from the WMD example, one would be at the point when people were scratching their heads and saying, "Why do we not have a bunch of folks get together and come up with a regime on missile technology? What would that look like?" For cybersecurity, some like-minded groups that can be brought together, perhaps based on a regional approach to the issue, would be the Asia-Pacific Economic Cooperation (APEC),[5] the International Multilateral Partnership Against Cyber

[5] See also http://www.apec.org/.

Threats[6] in Malaysia and the Organisation for Economic Co-operation and Development, all of which have done valuable work in this field.[7]

The Group of Eight (G8)[8] has a very important law enforcement cooperation process that addresses some of the operational difficulties for law enforcement purposes in cyberspace. Although using a letter rogatory, or a formal request from one country's court to a foreign court for judicial assistance, would take only about three months, evidence in cyberspace usually will last only 40 to 90 seconds. Again, another problem is distinguishing if it is a crime or an act of war, a determination that needs to be done in a matter of minutes. To address this, the G8 created 24-hour point of contact networks in about 16 countries, where a counterpart in one Justice Ministry can call on another counterpart and say: "I need help immediately. Can you help me?" The process may circumvent the diplomatic process, but it actually works pretty well.

If there are shared problems and like-minded countries, it might be easier to make progress on this. However, that does not mean that a global approach should not be undertaken.

Such an approach is interesting. If there are shared problems and like-minded countries, it might be easier to make progress. However, that does not mean that a global approach should not be undertaken. We have a global supply chain, a global network and a global community. This has to be addressed globally, but our report recommends a two-track approach, one based on like-minded nations and the other based on a global approach.

Norms are also important, but developing them will be difficult. A litmus test in some way is the Council of Europe Convention on Cybercrime.[9] If a State is a signatory, it would have taken the first step

[6] See also http://www.impact-alliance.org/index.html.

[7] See also http://www.oecd.org.

[8] The Group of Eight is a forum, created by France in 1975, for governments of six countries in the world: France, Germany, Italy, Japan, the United Kingdom, and the United States. Canada joined the group in 1976 and Russia in 1997. In addition, the European Union is represented within the G8, but cannot host or chair.

[9] The Convention on Cybercrime is the first international treaty seeking to address computer crime and Internet crimes by harmonizing national laws,

towards helping to secure cyberspace. For those that are not signatories, we should have questions. Developing norms would be difficult to separate from the Convention.

Why do I say this? Actually, I did not like the Convention. It was difficult for the United States to participate, having a different constitutional structure. After exceptionally long debates that lasted years, it decided in the end that it was better to have a common platform for law enforcement because the central problem was crime. Even when it is a State actor, a military problem or a security problem, one does not know if the culprit is a criminal, a State, or even a criminal acting on behalf of a State. Thus, important steps are reducing the scope of crime, shrinking the sanctuaries for criminals and increasing the spread of valuable laws that fully address cybercrime.

Progress is slow, but, for me, whether or not a State has endorsed the Convention is a very easy test of how serious it is about global cybersecurity. This may sound a bit harsh, but I want to emphasize the importance of this because, for this different kind of security problem, dealing with crime is essential. The classic approaches do not work.

I have participated in some discussions of the United States Department of Defense on cybersecurity. The fact that there is confusion within the Department's think tank, the National Defense University,[10] is an ominous sign. One difficult issue it struggles with is deterrence, especially in the face of a global network. Without knowing who is attacking, how can one deter them? In the film, *Dr. Strangelove*, a country built a doomsday machine but did not tell anyone because they were waiting to announce it on their national day. It thus had no deterrent effect. That has been similar to the American

improving investigative techniques and increasing cooperation among nations. The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature in Budapest on 23 November 2001 and entered into force on 1 July 2004. For the text of the Convention, see http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[10] The National Defense University is an institution of higher education funded by the United States Department of Defense, intended to facilitate high-level training, education, and the development of national security strategy. It is chartered by the Joint Chiefs of Staff and is located on the grounds of Fort Lesley McNair in Washington, D.C. See also http://www.ndu.edu/.

approach to cybersecurity for the last ten years. If one does not tell people what one plans to do, and if others do not know one's plans or who will be affected, deterrence is of limited value.

Another complicating problem for deterrence is that one could attack the wrong target. As I mentioned, the United States had almost mistakenly attacked another country for an incident in cyberspace carried out by teenagers in California. This happens all the time. In fact a shrewd attacker would be very careful to point to an innocent third party. A lot of times in the United States, people become excited and say that the Chinese are hacking them. I believe that if the trail of bread crumbs leads to Beijing, that is almost conclusive proof that the Chinese are not the perpetrators. It is a little more complicated. A good attacker would make it more difficult to determine his identity. How then would do one deter if one shoots at the wrong target?

Crucial for deterrence is also the involvement of third parties. The global, complex and highly populated shared network has led to the problem of collateral damage. This issue cannot be assessed in cyberspace; one cannot measure the extent of such damage. With a single global network, where an attack launched from one place will travel through many different networks on its way to its target, a counter-attack may also damage the intermediate third-party networks that are completely innocent. One of the questions that we have asked internally is how one can be assured that a counter-attack against a suspected State attacker will not accidentally bring down the University of California system.

Universities are very popular as a platform because of its numerous students and machines. Universities want to be open, thus making them attractive to hackers. It would be a very rash political leader who would authorize a counter-attack in cyberspace without being certain that it would strike the right target and not damage a third party. In fact, the United States is exceptionally distant from being in a position where it would ever authorize a counter-strike of this kind, without totally clear and undeniable evidence, which we hardly ever get.

So deterrence is not exactly a tool that is going to be useful. There are other ways to accomplish deterrence. In the end, this depends on changing the calculus of cost and benefits that the attackers are looking at. Right now, the formula is very much in the attackers' favor.

It is anonymous and low risk. Looking at this mainly as an espionage problem, one can acquire immense quantities of information at almost no cost, making this very attractive.

How do we change that? There's a couple of ways to change that. One way is to begin to shrink sanctuaries that currently exist. If a country hires a criminal to launch an attack, which we know has happened, we want to make it harder for those criminals to exist freely. There are places where the laws are inadequate for dealing with cybercrime. Laws need to be strengthened and a way to do that may be to adhere to the Council of Europe Convention on Cybercrime.

We need to make it harder for the attacker to benefit, the information harder to obtain and the infrastructure more robust. If the attacks become more costly and the benefits smaller, fewer attacks will occur. This is possible. Part of this will involve the development of norms. If the international community expresses its displeasure with a cyberattack, it will have a deterrent effect. We have not yet been able to do that, partly owing to the lack of well-defined norms. Norms would be useful, however if they exist in a vacuum, they would not actually do very much.

We can all think of situations where there are norms that are routinely flouted, but norms can be important for shaping behaviour. We need to look at the behaviour of States. Are they tolerating criminals? Have they signed up to the Cybercrime Convention? Do they use cyberattack as part of the portfolio of military activity? Behaviour is the indicator. In basketball, one is told to watch the person's waist, not his hands nor his mouth. It is the same for cyberspace—pay attention to the real indicators. Behaviour leads one back to attribution. Until we improve attribution, it will be very difficult to improve deterrence or enforce norms because we will not be able to clearly identify the responsible party. One can think of attacks where there have been allegations that they were State-sponsored and yet, there is no proof.

Regarding agreements and treaties, the first thing that might be useful to bear in mind is what we could call the asymmetry of risk. I think about it as some of the new arenas of conflict, the new domains for conflict. In the Cold War, risk was symmetrical. We had cities; they had cities. We had satellites; they had satellites. We had hostages; they had hostages. It was symmetrical. That encouraged deterrence and restraint. It encouraged at least an unspoken norm. None of that exists in cyberspace.

What we have in cyberspace is an asymmetry of risk. Some countries are what we would call "target-rich environments". The United States is the most target-rich environment because we are the most dependent on the Internet, through which it is possible to get access to advanced technology, research and nuclear weapons design. Other countries are almost as dependent on the Internet—in some ways it is linked to economic development, but not entirely—and more importantly, the whole world is moving in this direction. We are all becoming equally dependent. Ten or 15 years from now, the asymmetry of risk may not exist. However, at the moment the United States is much more vulnerable than its opponents, making it difficult to: (a) develop an adequate strategy; and (b) come up with both deterrence and agreements that are actually useful. I say useful because it needs to have a whole set of conditions associated with it. Again going back in some ways to the WMD precedent, the most important is how to verify compliance. Without this, the utility of an agreement is doubtful.

In addition to norms dealing with cybercrime and cooperation on building resiliency, another issue for international agreement is verification. An unverifiable agreement will be violated in this environment. Who will violate it? I do not know. It could be those teenagers in California again, or it could be someone else. It could be anyone. It could be States, criminals, teenagers or political activists. So, with no way to verify, enforce and ensure compliance, one is not going to get very much out of an agreement.

Another problem here is identifying the technologies that are involved in cyberconflict. There are no special or military technologies. One of those things that I find amusing is that 12 years ago, when I worked for the United States Government, we had some very exciting and advanced technologies for penetrating other people's networks, spending a huge amount of money in the process to develop such technology. People in northern Maryland would work for years on it, and within a few years of its deployment, it would be available on the black market. In fact, some items that can be bought from cybercriminal networks are as good as anything a State has. I have said to smaller countries, “Why do you bother doing this, just buy it from the criminals or hire them!” That is an option. Many have probably exercised it.

However, there is a community out there that is interested in thinking about how networks work. They are interested in thinking about the thrill of reading somebody else’s e-mail. They are interested in reaping the great financial rewards that come from cybercrime. The United States Department for Justice describes cybercrime now as the single best venue for bank robbery ever invented because one can rob a bank on another continent and have zero chances of being caught. One can take zero risk in the act and have zero risk in being caught.

So far, the advantage lies with these attackers.

Even legitimate, commercial products can have techniques and capabilities that are cause for worry. The famous example is Sony, which was worried about piracy. They put a piece of code into the devices they sold that would allow them to monitor what users were up to, so they could detect piracy. Cybercriminals discovered this Sony device within days of it being released and exploited it for criminal purposes. The problem is that we are facing an incredibly vibrant and innovative anonymous community.

This is a very difficult group to defend against right now. I believe that it is a virtual group, a community spread around the world. They may not know who they are because they are all using strange names like “hackerz” with a “z”, but they work together in thinking about how to defeat defences, overcoming security problems and penetrating networks. So far, the advantage lies with these attackers.

So if one thinks about how to verify an agreement on cybersecurity and how to make it truly meaningful, it would be very difficult due to the anonymity of the parties involved, which goes well beyond States. The technologies involved can be perfectly legitimate. They can be commercial and used for routine purposes. Unless one is willing to think about ways to control access to laptops, there will always be cybercrime and cyberespionage.

Appendix

Members of the Advisory Board on Disarmament Matters

Fifty-first session, 18-20 February 2009

Carolina Hernandez (Chair)
Founding President and Chair, Board of Directors
Institute for Strategic and Development Studies
Manila

Nobuyasu Abe
Director
Center for the Promotion of Disarmament and Non-Proliferation
Japan Institute of International Affairs
Tokyo

Anatoly I. Antonov
Director, Department for Security and Disarmament
Ministry of Foreign Affairs of the Russian Federation
Moscow

Dewi Fortuna Anwar
Director for Programme Research, Habibie Centre
Research Professor and Deputy Chairperson for Social Sciences
and Humanities of the Indonesian Institute of Sciences
Jakarta

Desmond Bowen
Former Director of Policy in the Ministry of Defence
London

Philippe Carré
Ambassador of France to Austria
French Embassy in Vienna

Jinye Cheng
Director-General, Department of Arms Control and Disarmament
Ministry of Foreign Affairs of China
Beijing

Kate Dewes
Co-Coordinator of the Disarmament and Security Centre
of the New Zealand Peace Foundation
Christchurch, New Zealand

Monica Herz
President, Brazilian Association of International Relations
Professor, Pontifical Catholic University of Rio de Janeiro
Rio de Janeiro, Brazil

Donald A. Mahley
Former Deputy Assistant Secretary for Threat Reduction,
Export Controls, and Negotiations
Bureau of International Security and Non-Proliferation
United States Department of State
Washington, D.C.

H.M.G.S. Palihakkara
Permanent Representative
Permanent Mission of Sri Lanka to the United Nations
New York

Olga Pellicer
Department of International Studies
Autonomous Technological Institute of Mexico
Mexico City

Adam Daniel Rotfeld
Former Minister of Foreign Affairs
Special Envoy of the Ministry of Foreign Affairs
Warsaw

Cheikh Sylla
Ambassador of Senegal to Germany
Embassy of Senegal
Berlin

Carlo Trezza
Special Envoy of the Italian Minister for Foreign Affairs
for Disarmament, Arms Control and Non-Proliferation
General Directorate for Multilateral Political Affairs and Human Rights
Ministry of Foreign Affairs
Rome

Theresa Hitchens (ex-officio member)
Director
United Nations Institute for Disarmament Research
Geneva