It should be noted that the articles contained in *Disarmament Forum*
are the sole responsibility of the individual authors.
They do not necessarily reflect the views or opinions of the United Nations,
UNIDIR, its staff members or sponsors.

Printed at United Nations, Geneva GE.07-01858—September 2007—4,440 UNIDIR/DF/2007/3 ISSN 1020-7287

TABLE OF CONTENTS

Editor's Note

Special Comment

ICTs and International Security

EDITOR'S NOTE

Information and communication technologies (ICTs) are embedded in every aspect of our lives—from the ability to communicate with Internet users around the world in real time, to the infrastructure that provides electricity to our homes and telephony to our office, to connecting our national security and defence networks. While global connectivity and development of ICTs have produced undeniable positive benefits, our reliance on ICTs and their ubiquitous nature have created new vulnerabilities.

There is increasing concern that these vulnerabilities can or will be exploited through cyberwarfare, cyberterrorism or attacks on critical information infrastructure. Yet there is little shared understanding of the terminology or definitions thereof among the range of actors—governments, the private sector, individuals, criminals, even terrorists—active in or concerned about these issues. Further, there are differing interpretations of whether the existing international legal framework is adequate in relation to acts of information warfare or cyberterrorism. A United Nations Group of Governmental Experts is expected to be convened in 2009 "to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them" (General Assembly resolution 60/45)—building on the initial efforts of the 2005 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

This issue of *Disarmament Forum* focuses on the civil and military threats posed by the use of ICTs for military, terrorist and political purposes that run counter to the maintenance of international security, and which could cause serious political, social and economic consequences. In order to encourage discussion, a wide range of perspectives on topics related to information security are presented herein. These include legal aspects of cyberspace and information warfare as they relate to national and international security; a discussion of cyberterrorism and Internet governance issues; how risks to critical information infrastructure can be analysed; and how various international and regional forums are addressing particular aspects of the information security issue.

The next issue of *Disarmament Forum* will focus on Central Asian security issues. After a period of being overlooked by many in the international community, Central Asia is once again at the centre of many security and development issues. While some refer to a renaissance of the Great Game, others stress the very contemporary security challenges faced by the region. Rich in resources, it is also a region of fragile states, disputed borders, resource conflicts and trans-regional threats.

"Central Asia at the Crossroads" will explore regional security interests, border and natural resource issues, small arms stockpiles, and sources of internal instability and conflict. It will look at how external influences are affecting the conflicting drives among Central Asian states to compete, or to cooperate, to resolve their security challenges.

From 17 May to 4 June 2007, the Security Needs Assessment Protocol (SNAP) project team travelled to Ghana to conduct a preliminary test of data generation techniques, to test ideas for field-team structure, and to learn about a variety of logistical aspects related to field missions. While in Ghana, SNAP conducted interviews with UN agency staff to learn about whether and how agencies assess community (beneficiary) security in the course of their work. The team also travelled to Ghana's Northern Region with eight local researchers to test key data generation techniques envisioned for the Security Needs Assessment Protocol. The objective was to learn about local terms, concepts and practices of security in a post-conflict environment.

On 4 and 5 June 2007, UNIDIR, the Program for the Study of International Organization(s) and Geneva Call held the conference Exploring Criteria and Conditions for Engaging Non-State Actors (NSAs) to Respect Humanitarian Law and Human Rights Law. Participants from UN agencies, academia and NGOs engaged in lively discussions on legal issues that relate to engaging NSAs in conflict and post-conflict situations.

In January 2006 UNIDIR launched a multi-phase research project on the international assistance offered to states for implementing the UN Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons (PoA). The first phase of the project culminated in the publication of a global overview of international assistance allocated between 2001 and 2005. The second phase of the project has included a series of case studies in the East African region with a view to establishing a mechanism to facilitate the matching of resources with needs. The report of the case studies is available on the UNIDIR web site (see UNIDIR Focus, page 54).

This phase of the project has also seen the development of a prototype of a web-based mechanism where National Focal Points in affected states will be able to post their self-identified assistance needs, and donors and implementing agencies will be able to pinpoint opportunities for cooperation in particular regions or thematic areas. Feedback on the prototype is being actively solicited and funding sought for the development phase.

The Secretary-General's Advisory Board on Disarmament Matters, which also serves as UNIDIR's Board of Trustees, met in New York from 16 to 18 July. This was the first meeting of the Board since the appointment of Secretary-General Ban Ki-moon. It was also the opportunity to welcome the new High Representative for Disarmament Affairs, Mr Sergio Duarte. The Advisory Board met under the able chairmanship of Ambassador Lee Ho-jin of the Republic of Korea.

In commemoration of the Tenth Anniversary of the entry into force of the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction and of the establishment of the Organisation for the Prohibition of Chemical Weapons (OPCW), UNIDIR, the OPCW, UN Office for Disarmament Affairs and the Pugwash Conferences on Science and World Affairs hosted a seminar on 7 August 2007 in Geneva. The panellists present the history of the negotiations of the Chemical Weapons Convention, the relevance of the CWC today and its current implementation status, with particular reference to the verification regime. The seminar also coincided with an exhibition presenting the implementation of the CWC and the work of OPCW.

Don't forget to check out the Disarmament Insight blog (see UNIDIR Focus, page 53)—www.disarmamentinsight.blogspot.com.

Kerstin Vignard

SPECIAL COMMENT

The last century has been characterized by dramatic changes with regard to scientific and technological developments. The multiplier effect and positive aspects of inventions in the area of information and communication technologies (ICTs) have become increasingly evident. ICTs facilitate communication, open new markets, attract investments and accelerate economic and social development. In an age of globalization, it is hard to imagine a country achieving economic prosperity without a well developed ICT infrastructure. The power of the ICT revolution rests with the fact that ICTs are embedded in every aspect of our lives—from communicating by e-mail and mobile phone to the command and control systems of our militaries.

However, while the benefits are innumerable, ICTs can also be used for malevolent or malicious purposes. There is increasing concern from many quarters about privacy issues, cybercrime, cyberterrorism and military use of information technologies.

While international debate and cooperation has moved forward on the first of these three areas to varying degrees, international understanding of ICTs and warfare is less developed. The Revolution in Military Affairs is founded on developments in ICTs, developments which have enabled military forces to assume new methods of command and control of personnel and equipment at the strategic and tactical levels. However, the evolution of ICTs also serves as a basis for cyberweapons and permits the possibility of electronic warfare. This has implications not only for changing forms and methods of conducting military operations, but could ultimately transform the traditional warfare paradigm, from physical battles between belligerents to information attacks in a virtual space that have all too real consequences in the physical world. As states come to terms with the capabilities—and dangers—of information warfare, it is not implausible that a cyberspace arms race could erupt. Such a race would not only be immensely destabilizing, but would also ultimately divert enormous resources from peaceful and sustainable development.

The potential threats posed by abuse of ICTs are of a universal and transnational character and touch upon all facets of the existence of states, societies, the private sector and individuals. However, despite the fact that these issues concern all of humanity, there are two major issues inhibiting international cooperation in this field. First, the terms used in discussion—such as information warfare, cybercrime, cyberterrorism, information weapons, information security, to name a few—lack agreed definitions. Second, there is a fundamental question about whether existing international law adequately covers security-related aspects of ICTs.

The international community has the responsibility not to allow this potential new area of confrontation among states to emerge. The United Nations has risen to the challenge through consideration by the General Assembly of the annual resolution on "Developments in the Field of Information and Telecommunications in the Context of International Security" initiated by the Russian

Federation in 1998 (resolution 53/70 of 4 December 1998). The resolution was adopted by consensus annually until 2005; for the past two years one state has voted against it.

The resolution stresses that ICTs and their means "can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security" and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields. The resolution also notes the necessity to "prevent the misuse or exploitation of information resources or technologies for criminal or terrorist purposes".

The resolution promotes consideration of existing and potential threats in the sphere of information security. It also encourages possible cooperative measures to address these threats and relevant international concepts aimed at strengthening the security of global information and telecommunication systems.

One of the first attempts to describe the spectrum of information security issues that are of primary importance for international community was made by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, which met in 2004 and 2005.

Continued interest in this topic was confirmed by resolution 60/45, which recommends the establishment in 2009 of "a group of governmental experts … to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them", as well as the concepts aimed at strengthening the security of global information and telecommunications systems.

I deeply appreciate UNIDIR's consistent support for international study and discussion of disarmament issues. Its interest in ICT security is long-standing, dating to its practical and positive initiative in convening an international meeting of experts in Geneva in August 1999 on developments in the field of ICT in the context of international security. This meeting helped to develop a better understanding of the substance of international information security issues and related concepts.

It is commendable that this issue of *Disarmament Forum* is dedicated to the subject of information security. This particular contribution will be a useful tool for diplomats, scientists, business, civil society and international organizations, as well as to the work of the 2009 Group of Governmental Experts on international information security.

Andrey Krutskikh

Chairman, United Nations Group of Governmental Experts on Developments in the Field
of Information and Telecommunications in the Context of International Security, 2004–2005

International information security: description and legal aspects

A.A. Streltsov

Intensive development of information and communication technologies (ICTs) and their wide use in all spheres of human activity have accelerated post-industrial development and the building of a global information society. ICTs have become a driving force of social development. The global information infrastructure provides unprecedented opportunities for communication among people, their socialization and access to information. Individuals, society and the state depend on the stability and reliability of the information infrastructure.

However, ICTs could enable a fundamentally new and effective means to disrupt or destroy a country's industry, its economy, social infrastructure and public administration. ICTs have the potential to be a means of combat capable of achieving goals related to inter-state confrontation at the tactical, operational and strategic levels.[1] In this way ICTs gain the characteristics of a weapon "designed to defeat an enemy in combat".[2] The potential destructive power of so-called "information weapons" will increase as ICTs develop further and as the information infrastructure of society evolves. This power will be magnified as military equipment and weapons are increasingly integrated with—and reliant on—ICTs.

These concerns are neither new nor limited to just one country or region. For example, the need to encourage the beneficial uses of ICTs and minimize the negative consequences was expressed in the 1998 joint statement of the Presidents of the Russian Federation and the United States "Common Security Challenges at the Threshold of the Twenty-First Century", which highlighted "the importance of promoting the positive aspects and mitigating the negative aspects of the information technology revolution now taking place, which is a serious challenge to ensuring the future strategic security interests of our two countries."[3]

Initial international efforts

Concerned about the emergence of new threats to peace and security, the Russian Federation has been promoting the issue of information security at the international level for nearly a decade. On 23 September 1998, I.S. Ivanov, Minister of Foreign Affairs of the Russian Federation, submitted a letter to the UN Secretary-General requesting circulation of a draft resolution on information security. A resolution entitled "Developments in the field of information and telecommunications in the context of international security" was then adopted by consensus at the Fifty-third Session of the General Assembly.[4]

A.A. Streltsov is Doctor of Engineering, Doctor of Law, professor, corresponding member of the Cryptography Academy of the Russian Federation, information security expert, and was a member of the Russian delegation at the meetings of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2004–2005).

The resolution called upon UN Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security. The resolution also invited all Member States to inform the Secretary-General of their views and assessments of the following issues:

- a general appreciation of the issues of information security;
- the definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunications systems and information resources; and
- the advisability of developing international principles that would enhance the security of global information and telecommunications systems and help to combat information terrorism and criminality.

The Secretary-General was requested to report to the Fifty-fourth Session of the General Assembly.

The report of the Secretary-General reflected the acknowledgement of the problem of international information security, as well as its complexity and multiple facets.[5] Based on submissions from Australia, Belarus, Brunei Darussalam, Cuba, Oman, Qatar, the Russian Federation, Saudi Arabia, the United Kingdom and the United States, the report highlighted the different priorities accorded by states to individual aspects of the issue as well as different approaches to the issue taken at the national and, especially, international levels.

Following this initial exploration of views, at the Fifty-fourth Session of the General Assembly the Russian Federation proposed a new draft resolution,[6] where for the first time the *military potential* of ICTs was by name put directly under the spotlight. This resolution was adopted without a vote on 1 December 1999.

In May 2000, with the objective of furthering discussion on the issue, the Russian Federation submitted to the UN Secretariat draft principles concerning international information security. These materials facilitated the adoption at the Fifty-fifth Session of the General Assembly of a resolution that noted the advisability of "examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems".[7]

In 2001, UN Member States agreed to establish a Group of Governmental Experts (GGE), commencing work in 2004, to review existing and potential threats in the field of international information security and possible measures to address them as well as to examine international concepts aimed at strengthening the security of global information and telecommunications systems.[8] Thus, for the first time at the international level, a political decision was made to move from discussion on the issue to practical action.

In April 2003 the Russian Federation submitted to the UN Secretariat a new contribution entitled "Issues Connected with the Work of the Group of Governmental Experts on Information Security", which contained the Russian vision of organizational, practical and substantial aspects of the group's work.[9] In particular, it was noted that it is necessary to seek a multilateral, mutually acceptable, international legal document aimed at strengthening the universal character of an international information security regime.

The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security met in 2004 and 2005, tasked with the preparation of a draft report for the UN Secretary-General. Even though the group undertook a substantial amount of work, it was unable to reach consensus on a draft report. The main stumbling block was the question of whether international humanitarian law and international law sufficiently regulate the security aspects of international relations in cases of "hostile" use of ICTs for politico-military purposes.

However, the work of the GGE was not in vain. It successfully raised the profile of the relevant issues on the international agenda. The preliminary exchange among states of their opinions on the most complicated aspects of these issues has been particularly fruitful. The importance accorded these topics is evident in the fact that the UN General Assembly has decided to continue studying this problem.[10] A new group of governmental experts will commence work in 2009.

Over the last 10 years, various aspects of the issue of information security have been taken under consideration in other international and regional forums, such as the International Telecommunication Union, the World Summit on the Information Society, and the Council of Europe. In addition to the resolutions mentioned above, the General Assembly has addressed other aspects of the ICT issue, such as creating a global culture of cybersecurity and the protection of critical infrastructures.[11]

International information security

Before addressing the question of whether existing norms of international law are sufficient to cope with the hostile use of modern ICTs, it is necessary to outline the area of study.

Information security is concerned with the threat of a state using ICTs to influence or attack the ICTs of another state. The hostile use of ICTs could generate situations considered as a threat to international peace and security.[12] Three aspects merit particular concern, each described briefly below.

Influencing and damaging another state's information resources and telecommunications systems using ICTs

These include:

- electronic attacks or information attacks through electronic impulses to temporarily or permanently neutralize electronic installations or systems;
- destroying or altering the operational algorithm of ICT control systems;
- influencing, disrupting or halting information or communication flows through interference with the signal distribution environment;
- spreading disinformation or creating a virtual picture partially or totally misrepresenting reality in the communications sphere; or
- producing disorientation, loss of will power or temporary destabilization among the population.

Deliberately influencing another state's vital structures

The use of ICT weapons would be particularly dangerous when used against military and civilian facilities and state systems and institutions, the disruption of the normal functioning of which could constitute a direct threat to national security.

Unauthorized penetration into control systems, for example that of a country's power grid, could bring about total paralysis of a country's infrastructure. Imagine the disastrous environmental risks if the chemical, biological or fuel industry were thus attacked, or the catastrophic consequences if a nuclear power station were involved.

Another critical sector is that of credit and finance. The unauthorized transfer or outright theft of bank resources, the "closing" of accounts and, in particular, mounting electronic attacks to block the computer networks of central banking institutions, could obviously not only create crisis situations in that particular area but also bring about the country's economic collapse or jeopardize its relations with other countries.

Massive destruction of the telecommunications infrastructure through the use of ICTs would amount to an attack on a state's control and decision-making systems.

An ICT attack on anti-aircraft, anti-missile and other defence communication and control systems would leave a state defenceless before a potential aggressor, thereby depriving it of the possibility to exercise its legitimate right of self-defence.

Targeting the communication, control and transportation systems of emergency response services could increase the loss of life and property in times of man-made or natural disaster.

Databases and other information resources of law enforcement bodies could be distorted or completely obliterated, which would gravely interfere with the fight against crime and the maintenance of law and order.

Undermining a state's economic and social systems and psychological manipulation of a population for the purpose of destabilizing society

The opportunities for carrying out massive attacks mean that ICTs could become a fundamental instrument of inter-state conflict.

The deliberate use of information to damage an opponent is hardly new. Today, however, owing to the widespread use of and reliance upon ICTs, the potential for such misuse has greatly increased. The opportunities for carrying out massive attacks mean that ICTs could become a fundamental instrument of inter-state conflict. As described in the contribution of the Russian Federation to the Secretary-General's 2001 report *Developments in the Field of Information and Telecommunications in the Context of International Security*:

> Pressure arising out of the predominance of a limited range of information sources might be used for the deliberate creation of a negative psychological effect on a country's population as a whole or on the staff of critically important structures, administrative and government services and legislative bodies.
>
> Causing people to feel unable to resolve their own problems, to mistrust the country's institutions or to feel hopeless, attacking their will power or provoking religious, ethnic or other conflicts undermines the foundations of the State and destabilizes society. Ultimately, such a situation could lead to antagonism between social groups, to civil war and to total disintegration of the State.[13]

Information warfare and international law

There is no doubt that information weapons can be used in practice. Some armed forces are already preparing special units for military operations using ICTs. The US Air Force, for example, has been quite open about its plans and is in the process of setting up a dedicated command—the Air Force Cyberspace Command.[14]

Further efforts by the international community to address the threat of hostile use of ICTs will depend on whether existing international law is seen as adequate to ensure international information security. This was affirmed by the 2004 International Expert Conference on Computer Network Attack and the Applicability of International Humanitarian Law,[15] and within the discussions of the UN Group of Governmental Experts in 2004 and 2005.

Ensuring international information security should be based on the principle of preserving existing international law (*jus ad bellum*), which regulates how threats to international peace and security are countered, and on international humanitarian law (*jus in bello*), which regulates the methods and means of warfare, protection of states that are not parties to the conflict, as well as of persons and objects that are or may be affected by the conflict.

In the international community's attempts to clarify this complex topic, there should be no attempt to diminish the legitimate right of self-defence of states to respond to hostile use of ICTs, just as they have the right to respond to a conventional weapon attack.

The UN Charter

The cornerstone of international law concerning the maintenance of international peace and security is the UN Charter, which stipulates, inter alia, that:

- all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations (Article 2.4);
- the Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security (Article 39);
- the Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures (Article 41);
- should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security (Article 42); and
- nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security (Article 51).

It is widely acknowledged by international law specialists that these rules establish a universal mechanism for maintaining international peace and security. However, now that ICTs are being developed or applied as a means of destruction (so-called "information weapons") and the international community has yet to arrive at a shared understanding concerning the place of information security within existing international law, the Charter could be interpreted in such a way as to provide international actors with a considerable degree of freedom to use ICTs to undertake aggressive actions and solve international disputes and conflicts.[16]

This strange set of circumstances stems from the fact that hostile actions in the information area have yet to be considered explicitly within international law on a par with hostile actions undertaken with traditional weaponry—even though the interconnectivity and dependence of today's world on ICTs mean that such an attack would be as devastating as a conventional attack—or perhaps even more so. Difficulties are further compounded by the lack of generally accepted interpretations as they apply to information security of such notions as "act of aggression" (Article 1), "force" (Article 2.4) and "armed attack" (Article 51).

Information attacks as an act of aggression

General Assembly resolution 3314 (XXIX) of 14 December 1974 defines an act of aggression.[17] Article 3 of the Annex to the resolution states:

> Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of article 2, qualify as an act of aggression:
>
> (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof,
>
> (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State;
>
> (c) The blockade of the ports or coasts of a State by the armed forces of another State;
>
> (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State;
>
> (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;
>
> (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State;
>
> (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein.

Although this resolution was not adopted by consensus, its "soft law" provisions provide the UN Security Council and all members of the international community with a benchmark for recognizing acts of aggression.

The use of an information weapon could be interpreted as an act of aggression if the victimized state has grounds for believing that the attack was conducted by the armed forces of another state and was aimed at disrupting the functioning of military facilities, destroying defensive and economic capacity or violating the state's sovereignty over a particular territory.

The issue of territory

In accordance with Article 41 of the UN Charter, among the measures available to the Security Council to give effect to its decisions include "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication", i.e. a blockade. However, traditionally a blockade is imposed along the external borders of a state, while today an information blockade could cross into the territory of a state, affecting every house, office, institution or business.

A cyber-blockade may be seen as interference in the internal affairs of a state, a violation of its sovereignty, or even a partial seizure of its national territory—actions which violate the international norm under consideration. This rule degenerates into farce if measures to impose and maintain an "information blockade" are implemented by a state's armed forces. In such a case the attacked state could invoke its inherent right of individual or collective self-defence, which implies the use of military force and conventional weapons.

Thus, the absence of a clear definition of "territory" in relation to cyberspace contributes to the gaps in international security law. Paragraph 4 of Article 2 of the UN Charter requires that all states shall refrain from the threat or use of force against the territorial integrity of another state. It is implied that there exists a physical territory subject to the state's jurisdiction and a formal border separating that territory from other states. However, there are no such concepts as national border and territory in the information sphere. A state could consider the entire global information infrastructure (or a portion thereof) to be its own territory, claim jurisdiction over the relevant elements of the information infrastructure and, on this basis, take action to defend these elements.

Identifying the attacker

Another complicating factor is how to reliably identify the agent of an information attack. It is technically challenging to localize the physical place from which such an act originates. But even if the origin of an attack can be localized within a particular state, it would be challenging to determine whether the attacker was acting in an individual capacity, or on behalf of a criminal organization, the government or armed forces. In such cases, the presumed perpetrator of an aggressive act could be falsely accused instead of truly identified, as recent events have shown.

Protecting critical infrastructure facilities

International law does not specifically cover the use of ICTs as a means of coercive pressure on an opposing state.

According to the Laws and Customs of War on Land introduced by the Hague Convention of 18 October 1907, "the attack or bombardment, by whatever means, of towns, villages, dwellings, or buildings which are undefended is prohibited."[18] Moreover, states party to the Convention are obliged to take "all necessary steps … to spare, as far as possible, buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided they are not being used at the time for military purposes."[19] These rules aim to alleviate the unnecessary suffering of the civilian population and the wounded as a result of military operations.

To be able to apply these provisions to cyberspace, it would be essential to be able to "mark" in some way the information systems used to maintain the viability of critical social infrastructure facilities: both for individual facilities (including military and civil hospitals, bomb shelters, etc.) and entire regions (water supply, electrical grids, dams, etc.). In the physical world, some of these facilities (such as hospitals) display a distinctive sign—the red cross or red crescent—indicating their protected status. Such identifying signs are absent in cyberspace, nor do criteria exist for designating these systems as critical infrastructure.

Perfidy

In relation to information warfare, the problem of preventing perfidy is one of the most urgent in international humanitarian law.

In accordance with Article 23 of the Hague Convention, belligerents are forbidden "to kill or wound treacherously individuals belonging to the hostile nation or army". Thus the spirit of chivalry should persist in relations between belligerents even during hostilities. The prohibition of killing or wounding the enemy in violation of this promise is the essence of this legal norm.

It would be reasonable to apply the same requirement to the behaviour of the parties to an inter-state conflict who launch ICT attacks on the civilian information infrastructure of another state. Commercial software and hardware used at infrastructure facilities are purchased with a certain guarantee of quality and security. An information attack would be facilitated if there were prepared "positions" in the software of ICT systems of the opposing party. These positions, for example, could be programs embedded in the software without the buyer's knowledge or consent. The incorporation of, for instance, malicious sleeping code or "backdoors" into such products is a deliberate breach of faith and a calculated violation of trust, and could be considered a form of perfidious behaviour. Acts of perfidy are already outlawed under international humanitarian law.[20]

Concluding suggestions

In conclusion, the international community has several areas to develop which would ultimately strengthen international information security. In the legal area, these include:

- determining the legality of the hostile use of ICTs;
- determining norms regulating operation, support and usage of the global information infrastructure;
- consolidating technical regulations in the field of information security and investigative procedures for identifying the perpetrator of an information attack;
- forbidding the use of ICTs to damage critical infrastructure facilities;
- establishing a system of "cyber identification" for critical infrastructure facilities;
- updating the belligerents' rules of behaviour to take into account the global information infrastructure and its infrastructural elements situated in neutral states;
- developing confidence measures in relation to commercially available software; and
- extending the prohibition of perfidy to commercial ICT products.

Notes

1. Deirdre Collings and Rafal Rohozinski, *Shifting Fire: Information Effects in Counterinsurgency and Stability Operations* (Workshop Report), United States Army War College 2006, p. 10.
2. Военный энциклопедический словарь [Military Encyclopedia], 1983, Moscow, Военное издательство, p. 523.
3. Signed in Moscow, 2 September 1998.
4. General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/53/70, 4 January 1999.
5. General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General,* UN document A/54/213, 10 August 1999.
6. General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/54/49, 23 December 1999.
7. General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/56/19, 7 January 2002.
8. Ibid.
9. This contribution, entitled "Issues Connected with the Work of the Group of Governmental Experts on Information Security", is contained within General Assembly, *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General,* UN document A/58/373, 17 September 2003, page 9.
10. General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/61/54, 19 December 2006.

11. See for example, General Assembly, Creation of a Global Culture of Cybersecurity, UN document A/RES/57/239, 31 January 2003; and General Assembly, Creation of a Global Culture of Cybersecurity and the protection of critical information infrastructures, UN document A/RES/58/199, 30 January 2004.
12. This section is based on the contribution of the Russian Federation to the Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security. See General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Secretary-General,* Addendum, UN document A/56/164/Add.1, 3 October 2001.
13. Ibid., Section 3, page 3.
14. See, for example, the 2006 statement of Secretary of the Air Force Michael W. Wynne, Cyberspace as a Domain in which the Air Force Flies and Fights, at <www.af.mil/library/speeches/speech.asp?id=283>.
15. Karin Bystrom (ed.), *Proceedings of the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law,* 17–19 November 2004, Stockholm, 2005.
16. Thomas C. Wingfield, *The Law of Information Conflict. National Security Law in Cyberspace,* Aegis Research Corporation, 2000.
17. General Assembly, Definition of Aggression, Resolution 3314 (XXIX), 14 December 1974.
18. Laws and Customs of War on Land (Hague IV), 18 October 1907, Article 25.
19. Ibid., Article 27.
20. Additional Protocol I of the Geneva Conventions, Article 37.

Critical information infrastructure: vulnerabilities, threats and responses

Myriam Dunn Cavelty

The recent Estonian–Russian "cyberbattle" has once again focused the world's attention on the topic of cyberspace security and critical information infrastructure protection (CIIP). When the Estonian authorities began removing a Second World War memorial—a bronze statue of a Soviet soldier—from a park at the end of April 2007, a three-week cyberbattle ensued, in which a wave of so-called Distributed Denial of Service attacks (DDoS) swamped various web sites—among them the web sites of the Estonian parliament, banks, ministries, newspapers and broadcasters—disabling the sites by overcrowding the bandwidths for the servers running the sites.

The Estonian–Russian online squabble made headlines[1] and various officials pounced on the cyberwar theme, following an unfortunate but frequently observable pattern of hyperventilation in cybersecurity matters.[2] It was claimed both explicitly and implicitly that the Russian Federation was behind the attack and that this was the first known case of one state targeting another by cyber-warfare.[3] One North Atlantic Treaty Organisation official reportedly said: "I won't point fingers. But these were not things done by a few individuals. This clearly bore the hallmarks of something concerted. The Estonians are not alone with this problem. It really is a serious issue for the alliance as a whole."[4]

A sober look at plain facts after the uproar reveals the usual pattern of such incidents: it is now clear that the "attacks" were not initiated by the Russian government or its security service. Fake Internet Protocol (IP) addresses—in this case, a Russian government computer was involved in the DDoS attack—are a routine part of any "hacktivist" attack.[5] Furthermore, the attacks were so low-tech and old-school that they were almost certainly carried out by large numbers of so-called script kiddies. These are teenagers with relatively little real computer expertise, who use readily available techniques and programs to search for and exploit weaknesses in other computers on the Internet. And finally, despite the fuss, the attacks had a relatively negligible effect (a usual feature of DDoS attacks).

There is an urgent need for such incidents to be considered in the right light, but fears connected to the risk of cyber-attacks cannot be entirely discounted as bogus. These fears, connected to the perception of the large-scale vulnerability of modern societies, have engaged the attention of security experts for a long time. This article will show how and why cybersecurity has come to dominate the *political* security debate at times over the last decade. It will look at the range of threats that seem to confront modern networked societies, set them into perspective and focus on obstacles and prerequisites of national and international protection measures.

Myriam Dunn Cavelty is head of the New Risks Research Unit at the Center for Security Studies at ETH Zurich, Switzerland and coordinator of the Crisis and Risk Network, see <www.crn.ethz.ch>.

The rise of CIIP to the political security agenda

Protection concepts for strategically important infrastructures and objects have been part of national defence planning for decades.[6] Today's concept of critical infrastructure protection (CIP), however, goes far beyond traditional national defence and military considerations. Its establishment as a focal point of the current national security debate is the result of two interlinked and at times reinforcing factors: the expansion of the threat spectrum after the Cold War, especially in terms of malicious actors and their capabilities; and a new kind of vulnerability due to modern society's dependence on inherently insecure information systems.

During the Cold War era, threats to national security mainly arose from the aggressive intentions of states to achieve domination over other states. The end of the Cold War brought the end of such clear, distinct threats: following the disintegration of the Soviet Union, a variety of "new" threats were moved onto the political security agendas of most countries.[7] These challenges have a quality of uncertainty about them: uncertainty concerning the entire range of "who, how, where, what, why, when".[8] Clearly, the understanding of "threat" as something imminent, direct and certain does not describe these challenges. Rather, they can be characterized as "risks", which are by definition indirect, uncertain and situated in the future.[9]

As a result of these diffuse risks and the difficulties of locating and identifying enemies, security policies have shifted away from focusing solely on actors, capabilities and motivations and toward looking at the general vulnerabilities of society as a whole as well. The United States military was a driving force behind the shaping of this threat perception in the early 1990s. As the only remaining superpower, the United States was considered predestined to become the target of asymmetric warfare, and those foes likely to fail against the US military might instead plan to bring the country to its knees by striking "soft targets" fundamental to the essential functioning of its entire society. These points are generally defined as critical infrastructure (CI). They are deemed critical because their incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of a state. Examples are telecommunications, power grids, transport and storage of gas and oil, banking and finance, traffic, water supply systems, emergency rescue services and public administration.

Fear of asymmetric measures against such targets has been aggravated by the so-called information revolution. Today, almost all CI relies on a spectrum of software-based control systems for smooth, reliable and continuous operation. In many cases, information and communication technologies (ICTs) have become omnipresent, connecting infrastructure systems and making them interrelated and interdependent. The part of the information infrastructure that is essential for the continuity of CI services is known as critical information infrastructure (CII). CII is thus part of a state's CI and includes components such as computers, software, the Internet, satellites and fibre optics.

CIIs are in general regarded as inherently insecure. Most of the components are developed in the private sector, where competition means that pressure to reduce time-to-market is intense, and where security does not drive system design. Computer and network vulnerabilities are therefore to be expected, and these lead to information infrastructures with in-built instabilities and critical points of failure.[10] Moreover, many researchers agree that the infrastructure is its own worst enemy because of its complexity.[11] Systems begin to blend into one another due to increasing use of ICTs and increasing functional demands and it is useless to try to maintain a separation of systems, each with an internally demarcated mode of responsibility. The distinction between inside and outside the system, and even the concept of systems boundaries as such, becomes blurred. Attacking infrastructure therefore has a "force-multiplier" effect that allows even a relatively small attack to achieve a great impact.[12] The spread of ICT appears to make the post-Cold War asymmetric threat easier; facilitating access to the tools for attack, and making the success of an attack more likely. Borders, which are already porous in the real world, are non-existent in cyberspace.

The threat to CII

As most critical infrastructure is either based on or monitored and controlled by vulnerable ICT systems, the information infrastructure became *the* focal point of CI protection policies in the 1990s.[13] Today, the information infrastructure is still regarded as an easy and vulnerable entry point. But discovering the threat to CII—the perpetrators, the likely nature of an attack—remains difficult.

The spectrum of potential perpetrators ranges from teenagers (the script kiddies described above), to sophisticated, expert hackers and crackers, to criminals, terrorists and even nation states. Since it would seem peculiar to cast all of these actors into the same pot, they are sometimes separated into two groups, based on organizational complexity, motivation and resources, albeit with fluent boundaries: the first group is considered to be an "unstructured" threat, the second a "structured" threat.[14]

The unstructured threat is random and relatively limited. It consists of adversaries with restricted funds and organization and short-term goals, such as individual hackers and crackers as well as small groups of organized criminals. The resources, tools, skills and funding available to the actors are too limited to accomplish a sophisticated attack against CI and, more important, the actors lack the motivation to do so. They do it for thrill, prestige or monetary gain. In contrast, structured threats are considerably more methodical and better supported. Adversaries from this group have extensive funding, organized professional support and access to intelligence products, and long-term strategic goals. Foreign intelligence services, well organized terrorists, professional hackers involved in information warfare, larger criminal groups and industrial spies fall into this threat category.

Unfortunately, there are no clear boundaries between the two categories. Even though an unstructured threat is not usually considered of direct concern to national security, there is a possibility that a structured threat actor could masquerade as an unstructured threat actor, or that structured actors could seek the help of technologically skilled individuals from the other group. While ordinary hackers lack the motivation to cause violence or severe economic or social harm,[15] it is feared that an individual with the capability to cause serious damage but lacking motivation could be swayed by sufficiently large sums of money to provide knowledge to more malicious actors.

The global nature of information networks means that attacks can be launched from anywhere in the world, so discovering the origins of an attack remains a major difficulty, if indeed the attack is detected at all. The problem of identifying actors is made particularly complicated by time lapses between an intruder taking action, the intrusion itself and the effects of the intrusion. Methods of attack have also become more sophisticated, even automated in parts, resulting in greater damage from a single attack. Furthermore, technology develops extremely quickly: the time between the discovery of a new vulnerability and the emergence of a new tool or technique that exploits that vulnerability is getting shorter. Indeed, the technology employed in many attacks is simple to use, inexpensive and widely available on computer bulletin boards and various web sites, as are encryption and anonymity tools. Without doubt, cyberthreats fall into the category of "new" challenges: indirect, and all too uncertain.

Cyberterror? Unlikely

Not surprisingly, the attacks of 11 September 2001 strengthened the general CIP debate's focus on terrorism, including cyberterrorism. The media is fascinated by the "cyber-" prefix in connection with disaster, and routinely features sensationalist headlines.[16] For their part, experts and government officials also frequently warn about cyberterrorism as a looming threat to national security. This creates a strange circle of news generation: the evidence that is presented in hearings is often based on (true or false) stories in the media; the media then quote these government officials' statements.

"Cyberterrorism" plays on two fears of the unknown: of the power of computer technology and of random and violent victimization.[17] A highly emotive word then, and frequently misused, although the fears that it invokes make a concise definition and accurate usage all the more important. Only attacks that are carried out by terrorists, which instil fear by effects that are destructive or disruptive, and which have a political, religious or ideological motivation, should fall under the term cyberterrorism.[18]

According to this definition, none of the disruptive incidents that we have seen so far qualify as examples of cyberterrorism. In fact, even though most terrorist groups have seized on the opportunity accorded by the information revolution to establish a multiple web presence for recruitment and fundraising purposes, as well as the dissemination of uncensored propaganda,[19] cyberspace has so far mainly served terrorists as a force multiplier in intelligence gathering and target acquisition, and not as an offensive weapon. And, in the eyes of some experts, it is unlikely to emerge as a weapon of choice.[20] So although we cannot afford to shrug off the threat altogether, because of the rapid progress of technological development and changes in the capabilities of terrorist groups,[21] decision makers as well as experts must be very careful not to foment "cyber-angst" and add to the hype that is clouding the issue.

The infrastructure of modern societies is vulnerable to all kinds of threats and risks, and terrorism is neither the most likely nor the most dangerous in terms of damage. Risks from natural disasters, mechanical failure and the inadvertent actions of an authorized user are just as serious as the risk of deliberate attack. The complexity of CII means that even planned maintenance operations, despite careful assessment and approval procedures, can cause disruptions. Clearly, the entire CIIP debate can only benefit if it moves away from focusing too much on malicious attacks and toward the far broader range of potentially dangerous events, including failure due to human error or technical problems. This not only does justice to the many facets of the security problem, but also prevents us from carelessly invoking the term terrorism.

The entire CIIP debate can only benefit if it moves away from focusing too much on malicious attacks and toward the far broader range of potentially dangerous events.

CIIP: toward an all-hazard approach and a resilience strategy

Comprehensive protection of the entire critical infrastructure against all threats and risks is impossible, not only for technical and practical reasons, but also because of costs. So the greatest vulnerabilities need to be identified; those structures that are more critical, or vital points within the infrastructure. Criteria could also focus on the relative likelihood of the threat or the relative cost of protection. But when considering actual protection measures, all of these require knowledge of the nature of the threat: it makes a difference whether one needs to protect a facility against a group of well trained attackers or whether one wants to shield information systems from unauthorized access. There is no one-fits-all solution: protection measures have to be tailored to specific assets and specific threats.

For as long as there are no reliable data on the likely nature of threats, another approach promises better results. This focuses on the likely *effects* of a failure of a specific infrastructure or asset and seeks to mitigate them. The reasoning for this is quite simple, especially for CII: from the perspective of maintaining reliable services, it is not so important whether the events that triggered the surprise originated from within or outside the infrastructure. In practice, it is in fact often difficult to determine whether a particular detrimental event is the result of a malicious attack, a component failure or an accident.[22] The first and most important question is not what caused the loss of information integrity, but rather what the possible result and complications may be. A power grid might fail because of a simple operating error without any kind of external influences, or because of a sophisticated hacker attack. In both cases, the result is the same: a possible power outage that may set off a domino effect of successive failures in interlinked systems. Analysing whether a failure was caused by a terrorist, a criminal, simple human error or spontaneous collapse will not help to stop or reduce the effect.

It is therefore beneficial to follow an "all hazards" approach, designed for protection efforts irrespective of the nature of the threat, with a focus on the capability to respond to a whole spectrum of unanticipated events. The key is to create greater resilience, commonly defined as the ability of a system to recover from adversity and either revert to its original state or assume an adjusted state based on new requirements.[23] Most precautionary and response measures can be employed as protection against both deliberate and natural surprises, except for the activities of the intelligence services and certain police and military responsibilities (such as physical protection), which are all geared toward actor-induced threats.[24]

Need for cooperation with the private sector

An all hazards approach, indeed any CIIP policy,[25] requires cooperation: when it comes to providing security for their citizens, governments can no longer go it alone. In many countries, the provision of energy, communications, transport, financial services, etc. have been, or are being, privatized.[26] Thus ownership, operation and supply of CII are largely in the hands of the private sector. Collectively, the private sector has far more technical resources and operational access to CII than the government.[27] But it has not used these resources to maximize security: satisfying shareholders by maximizing company profits has often led to minimal security measures. The government, however, wants industry to take responsibility for implementing protection measures in line with the parameters or frameworks set by public authorities.[28] In order to gain the support of the private sector without having to introduce heavy regulation, governments must strive to create a mutual win–win situation.

Luckily, states can provide a number of services that are of interest to the private sector. Clearly, CII operators know their business better than any governmental unit and usually have many other sources from which to obtain warnings or advice. However, a state-run CIIP unit would be able to provide non-technical analyses of the general risk situation prepared by national and international intelligence services, such as information about the nature of criminal organizations. Also, the private sector could gain knowledge about incidents and lessons learned by an exchange with other private actors mediated by a "neutral" government entity.[29] Further, states can provide financial assistance, through funding research on protection technologies and contributing to implementation costs.[30]

Global issue, global response

National efforts can only go so far: the vulnerability of modern societies—caused by their dependence on a spectrum of highly interdependent information systems—has global origins and implications. The information infrastructure transcends territorial boundaries, so that information assets that are vital to the national security and the essential functioning of the economy of one state may reside on the territory of other states. Additionally, cyberspace—a huge, tangled, diverse and almost ubiquitous web of electronic interchange—is present wherever there are telephone wires, cables, computers or electromagnetic waves, a fact that severely curtails the ability of individual states to regulate or control it alone. Any adequate protection policy that extends to strategically important parts of the information infrastructure will thus require transnational solutions.

However, an underlying tension concerning the use of cyberspace has been partly responsible for preventing the coherent establishment and implementation of rules and norms at the international level.[31] Some states are developing doctrines and even capabilities to exploit cyberspace for military advantage: they are investing in military technologies and doctrines designed to disrupt the (information) infrastructure of rival states. The offensive and aggressive use of cyberspace, and initiatives to protect cyberspace from aggressors, are being pursued simultaneously.[32] Due to this, there have been calls for efforts to control computer exploitation by state militaries through arms control or multilateral behavioural norms, agreements that might pertain to the development, distribution and deployment of cyberweapons, or to their use.[33] However, traditional capability-based arms control will clearly not be of much use, mainly because it is impossible to verify any such controls. Structural approaches, attempts to prohibit the means of information warfare altogether or to restrict their availability, are largely unfeasible because of the ubiquity and dual-use nature of information technology.[34] The avenues available for arms control in this arena seem primarily information exchange and norm-building, and even these are only being pursued to a limited degree.

Although there may be tensions regarding the use of cyberspace, and traditional arms control cannot meet the challenges posed by information technology, other international approaches are more promising. One key issue for all states is the harmonization of law to facilitate the prosecution of perpetrators of cybercrime. Cybercrime is considered a menace to the economic prosperity and social stability of all states that are plugged into the global information infrastructure. All states therefore have an interest in working together to devise an international regime[35] that will ensure the reliability and survivability of information networks. Again, this is more of a resilience strategy than a threat-focused approach. Multilateral conventions on computer crime, such as the Council of Europe's Convention on Cybercrime (2001), could be expanded and built on. International organizations could help develop and promulgate information security standards and disseminate recommendations and guidelines on best practices. International law enforcement institutions and mechanisms, like Interpol, could be used for information exchange—in order to provide early warning of any attack—and cybercrime investigations. Enhanced cooperative policing mechanisms could also be created.

It is key, however, not to duplicate efforts already undertaken at national level or below: the principles of subsidiarity and proportionality must be taken into account at all times. Activity at the international level should concentrate on challenges that cannot be mastered by a state or region on its own, such as global infrastructures, like the Internet, or truly large-scale interdependencies. By taking such steps, international organizations can help to strengthen the complex and at times overlapping web of national and regional initiatives in the realm of CIIP, and can improve the security and dependability of systems, management practices and international policing efforts.

Cooperation: the key to CIIP

The protection of critical information infrastructure has reached the international political security agenda. Cyberterror is often mentioned in relation to these threats, but the menace in fact ranges far wider, from more straightforward crime to natural disaster and even basic human error. But comprehensive protection against the entire range of threats and risks at all times is near impossible, not only for technical and practical reasons, but also because of the associated costs. What is possible is to focus protective measures on preventive strategies and on trying to minimize the impact of an attack when it occurs.

Because it is mainly infrastructure providers that are in the position to install technical safeguards for information technology security at the level of individual infrastructures, national governments depend on cooperation with the private sector to provide the public good of security to their citizens. But national protection measures only go so far: the securing of the global information infrastructure is a global task. Currently, divergences between national CIIP policies are a major obstruction to the development of an international regime, for international regimes are based on at least a minimal convergence of expectations and interests of (national) key actors. However, in consideration of their economic and security interests, industrialized states are working to overcome these temporary obstacles in order to move resolutely toward robust international conventions and mechanisms that protect the global information environment.

Notes

1. See, for example, "Cyberattack on Estonia Stirs Fear of 'Virtual War'", *International Herald Tribune,* 18 May 2007, at <www.iht.com/articles/2007/05/18/news/estonia.php>; "The Cyber Raiders Hitting Estonia", *BBC News,* 17 May 2007, at <news.bbc.co.uk/1/hi/world/europe/6665195.stm>; "Estonia Urges Firm EU, NATO Response to New Form of Warfare: Cyber-attacks", *The Sydney Morning Herald,* 16 May 2007, at <www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html>.
2. Myriam Dunn Cavelty, forthcoming 2007, *Cyber-security and Threat Politics: US Efforts to Secure the Information Age,* London, Routledge.
3. "Russia Accused of Unleashing Cyberwar to Disable Estonia", *The Guardian,* 17 May 2007, at <www.guardian.co.uk/frontpage/story/0,,2081512,00.html>.
4. Ibid.
5. Hacktivism stands for the marriage of hacking and activism, and describes operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are web "sit-ins" and virtual blockades, automated e-mail bombs, web hacks, computer break-ins, and computer viruses and worms. See Dorothy E. Denning, 2001, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", in J. Arquilla and D. Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy,* Santa Monica, CA, RAND, pp. 239–288.
6. Eric A.M. Luiijf, Helen H. Burger and Marieke H.A. Klaver, 2003, "Critical Infrastructure Protection in the Netherlands: A Quick-scan", in Urs E. Gattiker, Pia Pedersen and Karsten Petersen (eds), *EICAR Conference Best Paper Proceedings 2003,* at <www.crypto.rub.de/imperia/md/content/lectures/kritis/bpp_13_cip_luiijf_burger_klaver.pdf>.
7. B. Buzan, O. Wæver and J. de Wilde, 1998, *Security: A New Framework for Analysis,* Boulder, CO, Lynne Rienner.
8. E.O. Goldman, 2001, "New Threats, New Identities, and New Ways of War: The Sources of Change in National Security Doctrine", *Journal of Strategic Studies,* vol. 24, no. 2, p. 45.
9. J. van Loon, 2000, "Virtual Risks in an Age of Cybernetic Reproduction", in B. Adam, U. Beck and J. van Loon (eds), *The Risk Society and Beyond: Critical Issues for Social Theory,* London, Sage, pp. 165–182.
10. Michael Näf, 2001, "Ubiquitous Insecurity? How to 'Hack' IT Systems", *Information & Security: An International Journal,* no. 7, pp. 104–118.
11. M.J.G. van Eeten, E.M. Roe, P. Schulman and M.L.C. de Bruijne, 2006, "The Enemy Within: System Complexity and Organizational Surprises", in M. Dunn and V. Mayer (eds), *International CIIP Handbook 2006. Vol. II: Analyzing Issues, Challenges, and Prospects,* Zurich, Center for Security Studies at ETH Zurich, at <www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16157>, pp. 89–109.
12. Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, Threat Analysis No. TA03-001, 12 March 2003, at <www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf>.
13. The attacks of 11 September 2001 highlighted the fact that terrorists could cause enormous damage by attacking critical infrastructures directly and physically and thus demonstrated the need to re-examine physical protections as well. See J.D. Moteff, 2003 (updated 13 March 2007), *Critical Infrastructures: Background, Policy, and Implementation,* Congressional Research Service report RL30153, Washington, DC, at <www.fas.org/sgp/crs/homesec/RL30153.pdf>, p. 3.
14. National Research Council, 1991, *Computers at Risk: Safe Computing in the Information Age,* Washington, DC, National Academy Press; Kenneth A. Minihan, Director, National Security Agency, Statement to the Senate Governmental Affairs Committee on Vulnerabilities of the National Information Infrastructure, at <www.senate.gov/~gov_affairs/62498minihan.htm>, 24 June 1998.
15. Dorothy E. Denning, 2002, "Is Cyber Terror Next?", in Craig Calhoun, Paul Price and Ashley Timmer (eds), *Understanding September 11,* New York, W.W. Norton, at <www.ssrc.org/sept11/essays/denning.htm>.

16. See, for example, "Bracing for Guerrilla Warfare in Cyberspace", *CNN Interactive,* 6 April 1999; "Terror Groups Hide behind Web Encryption", *USA Today,* 5 February 2001; "Suspect Claims Al Qaeda Hacked Microsoft – Expert", *Newsbytes,* 17 December 2001; "FBI: Al Qaeda May Have Probed Government Sites", *CNN,* 17 January 2002; "Islamic Cyberterror. Not a Matter of If But of When", *Newsweek,* 20 May 2002.
17. M.M. Pollitt, "Cyberterrorism – Fact or Fancy?", *Proceedings of the 20th National Information Systems Security Conference,* October 1997, pp. 285–289.
18. Maura Conway, 2002, "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet", *First Monday,* vol. 7, no. 11, <firstmonday.org/issues/issue7_11/Conway>; Myriam Dunn Cavelty, forthcoming 2007, "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate", *Journal of Information Technology and Politics,* vol. 4, no. 1.
19. Timothy L. Thomas, 2003, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters,* spring, pp. 112–123; Gabriel Weimann, 2004, *www.terror.net. How Modern Terrorism Uses the Internet,* United States Institute of Peace, Special Report 116; Gabriel Weimann, 2004, *Cyberterrorism—How Real Is the Threat?* United States Institute of Peace, Special Report 119.
20. S. Barak, 2004, "Between Violence and 'E-jihad': Middle Eastern Terror Organizations in the Information Age", in L. Nicander and M. Ranstorp (eds), *Terrorism in the Information Age – New Frontiers?* Stockholm, Swedish National Defence College, pp. 83–96.
21. Institute for Security Technology Studies, Technical Analysis Group, 2004, *Examining the Cyber Capabilities of Islamic Terrorist Groups,* Dartmouth College, NH, at <www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf>.
22. R.J.Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T. Longstaff, and N.R. Mead, 1997 (updated 1999), *Survivable Network Systems: An Emerging Discipline,* technical report CMU/SEI-97-TR-013, ESC-TR-97-013, at <www.cert.org/research/97tr013.pdf>, p. 3.
23. John A. McCarthy, 2007, "Introduction: From Protection to Resilience: Injecting 'Moxie' into the Infrastructure Security Continuum", in *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience,* CIP Program Discussion Paper Series, Washington, DC, George Mason University, at <cipp.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf >, pp. 2–3.
24. Sergio Bonin, 2007, *International Biodefense Handbook 2007: An Inventory of National and International Biodefense Practices and Policies,* Zurich, Center for Security Studies at ETH Zurich, p. 378.
25. I. Abele-Wigert and M. Dunn, 2006, *International CIIP Handbook 2006. Vol. I: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies,* Zurich, Center for Security Studies at ETH Zurich.
26. Jan Joel Andersson and Andreas Malm, 2006, "Public-Private Partnerships and the Challenge of Critical Infrastructure Protection", in M. Dunn and V. Mauer (eds), op. cit., pp. 139–167.
27. Z. Baird, 2002, "Governing the Internet: Engaging Government, Business, and Nonprofits", *Foreign Affairs,* vol. 81, no. 6, pp. 15–20.
28. Seymour E. Goodman, Pamala B. Hassebroek, Daving Kind and Andy Azment, 2002, *International Coordination to Increase the Security of Critical Network Infrastructures,* document CNI/04; Olivia Bosch, 2002, *Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection,* both papers presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures, Seoul, 20–22 May 2002.
29. Center for Security Studies at ETH Zurich, 2006, *Information Security in Swiss Companies: A Survey on Threats, Risk Management and Forms of Joint Action,* Zurich; Manuel Suter, 2007, *A Generic National Framework For Critical Information Infrastructure Protection,* paper presented at the ITU 2nd Facilitation Meeting for WSIS Action Line C5: Building Confidence and Security in the Use of ICTs, at <www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf>.
30. I. Abele-Wigert and M. Dunn, op. cit., pp. 385–402.
31. A. Rathmell, 2001 "Controlling Computer Network Operations", *Information & Security: An International Journal,* no. 7, pp. 121–144.
32. Ibid.
33. Heinrich Böll Stiftung, 2001, *Perspectives for Peace Policy in the Age of Computer Network Attacks,* Conference Proceedings, at <www.boell.de/downloads/medien/DokuNr20.pdf>; Dorothy E. Denning, 2001, *Obstacles and Options for Cyber Arms Controls,* paper presented at Arms Control in Cyberspace Conference, Heinrich Böll Foundation, Berlin, 29–30 June 2001, at <www.cs.georgetown.edu/~denning/infosec/berlin.doc>.
34. Ibid.
35. A regime can be defined as "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations". See Stephen D. Krasner (ed.), 1983, *International Regimes,* Ithaca, NY, Cornell University Press, p. 2.

Terrorism and Internet governance: core issues

Maura Conway

Global governance is a vast and complex issue area in itself, and the subset of issues that may be termed "Internet governance" are equally so. The difficulties of trying to "legislate" at the global level—efforts that must encompass the economic, cultural, developmental, legal and political concerns of diverse states and other stakeholders—are further complicated by the technological conundrums encountered in cyberspace. The unleashing of the so-called global war on terrorism complicates things yet further. Today, both substate and non-state actors are said to be harnessing—or preparing to harness—the power of the Internet to harass and attack their foes. International terrorism had already been a significant security issue prior to 11 September 2001 and the emergence of the Internet in the decade before. Together, however, the events of 11 September and advances in information and communication technologies have added new dimensions to the problem. In newspapers and magazines, in film and on television, and in research and analysis, "cyberterrorism" has become a buzzword. Since the events of 11 September 2001, the question on everybody's lips appears to be "is cyberterrorism next?" It is generally agreed that the potential for a "digital 9/11" in the near future is not great. This does not mean, however, that scholars of international relations may continue to ignore the transformative power of the Internet.

This paper explores the difficulties of Internet governance in the light of terrorists' increasing use of the medium. In particular, it details the clampdown on the burgeoning Internet presence of extremist groups undertaken by both state-based and substate actors in the wake of the attacks of September 2001 in the United States and of July 2005 in the United Kingdom. The challenges of governance are many and varied, but include:

- debates over the role of various actors in the governance process, including national governments, hacktivists, and Internet service providers (ISPs);
- the appropriate legislative response to the terrorist Internet presence; and
- the debate over free speech versus limits on speech.

The description and analysis of these challenges are at the centre of this paper. First, however, it is worth considering what exactly is meant by the term "Internet governance".

Maura Conway is a lecturer in the School of Law and Government at Dublin City University, Ireland. Her principal research interests are in the area of terrorism and the Internet, including academic and media discourses on cyberterrorism, and the functioning and effectiveness of terrorist web sites. An extended version of this article, "Terrorism, the Internet, and International Relations: the Governance Conundrum", is to be published in M. Dunn, V. Mauer and F. Krishna-Hensel (eds), forthcoming 2007, *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace,* London, Ashgate.

What is meant by "Internet governance"?

The Internet had unique governance structures during its development and early growth. It began life as a government project: in the late 1960s, the United States government sponsored the establishment of the Defence Advanced Research Projects Agency, which was charged with developing a resilient communication facility designed to survive a nuclear attack. By the 1980s, a wider community was using the facilities of this network, which had come to be referred to as the Internet. In 1986, the Internet Engineering Task Force was established to manage the further development of the Internet through a cooperative, consensus-based decision-making process involving a wide variety of individuals. However, in 1994, the US National Science Foundation decided to involve the private sector by subcontracting the management of the Domain Name System (DNS) to Network Solutions. This angered many end-users and resulted in a dispute, which was only resolved in 1998 with the establishment of a new international organization, the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit public-private partnership dedicated to preserving the operational stability of the Internet via broad representation of global Internet communities through bottom-up, consensus-based processes.

Since the establishment of ICANN, however, the debate on Internet governance has been characterized by the more direct involvement of national governments, mainly through the United Nations framework and institutions. The first World Summit on the Information Society (WSIS), held in Geneva in December 2003, officially placed the question of Internet governance on diplomatic agendas. The Declaration of Principles and the Plan of Action adopted at WSIS 2003 proposed a number of actions in the field of Internet governance, including the establishment of a Working Group on Internet Governance (WGIG).[1] This became necessary because both "Internet" and "governance" were the subject of controversy, as was the concept of "Internet governance" itself.

"Governance" was the subject of particular controversy, especially during the WSIS. Misunderstandings stemmed from terminological confusion. When the term "Internet governance" was introduced in the WSIS process, many countries linked it to the concept of government. One of the consequences was the belief that Internet governance issues should be addressed primarily at the intergovernmental level with only limited participation from other actors. What were the main reasons for this terminological confusion? Gelbstein and Kurbalija argue that it is not necessarily obvious to many that the term "governance" does not mean "government". They point out, for example, that the term "good governance" has been used by the World Bank to promote the reform of states by introducing more transparency, reducing corruption and increasing the efficiency of administration and that, in this context, the term "governance" was directly related to core government functions.[2]

In his analysis of Internet governance, Klein draws on Robert Dahl's seminal text *Democracy and Its Critics* (1989), in which Dahl identifies what he views as the minimal conditions necessary for the establishment of an effective system of governance: authority, law, sanctions and jurisdiction. "These four mechanisms make governance possible: the governing *authority* can make a policy decision that applies within its *jurisdiction*, embodying that decision in *law* and imposing *sanctions* on whomever disobeys" [italics in original].[3] Dahl's conception of governance is closer to "government" than perhaps many of those connected with the development of the Internet—other than national governments—might find acceptable. Indeed, the WGIG has since published the following working definition of Internet governance: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[4] This does not mean that the four issues identified by Dahl are of no importance—they arise repeatedly in any discussion of the relationship between terrorist use of the Internet and Internet governance;

what the WGIG definition does draw our attention to, however, is the legacy of the early years of the Internet's development and the resulting importance of actors other than states in the Internet governance process.

Terrorism and the Internet: a brief history

In a little over four weeks in April and May 2004, the now-deceased Abu Musab al-Zarqawi, one-time leader of Al-Qaeda in Iraq, "rocketed to worldwide fame, or infamy, by a deliberate combination of extreme violence and Internet publicity".[5] In early April 2004, al-Zarqawi posted online a 30-minute audio recording which explained who he was, why he was fighting and details of the attacks for which he and his group were responsible. Prior to the instigation of this Internet-based public relations campaign, each of al-Zarqawi's attacks had to kill large numbers of people in order to get noticed in the chaos and mounting daily death toll in Iraq. By going online, however, al-Zarqawi was able both to control the interpretation of his violent actions and achieve greater impact with smaller operations.

In May 2004, al-Zarqawi took things a step further and used the Internet's force-multiplying power to maximum effect when he was filmed cutting off the head of a US hostage and had the footage posted online.[6] The purpose of this video was to create images that would grab the attention of allies and enemies alike. In this respect, it was an undoubted success; al-Zarqawi risked very little in this undertaking, but accomplished "as much if not more to undermine US plans as a bomb that killed 100 people in Najaf. And [at the same time] made himself a hero to jihadis across the world."[7] The free availability of this and other grisly "snuff movies" on the Internet led to a realization that the most important aspect of the terrorism–Internet relationship was not the much discussed cyberterrorism, but those more mundane and everyday terrorist uses of the Internet, from information provision to recruitment, which have a history stretching back for many years before al-Zarqawi's appearance.

Today, virtually every active militant group has an online presence, and many groups are the subjects of more than one site. A number of these groups have already shown a clear understanding of the power of the global information network to publicize their position: Lebanese Hizbollah has clearly demonstrated this ability, as have the Tamil Tigers and Al-Qaeda. Unsurprisingly, in the post-11 September world, the latter are subject to much increased scrutiny. The remainder of this paper is concerned with describing and analysing the attempts at Internet governance instigated by those with concerns about increasing extremist use of the Internet for the purposes of, among other things, information dissemination and thence recruitment: much is therefore concerned with what is called content control, efforts on the part of stakeholders to regulate what sort of material is available on the Internet.

Content control issues

Who is responsible for content policy?

When it comes to terrorism, governments are generally held to be the main players in the area of content control, as they prescribe what should be controlled and how. Some groups of individual users, such as hacktivists, are also keen to play their part, however, and indeed have had some success in disrupting the online presence of a number of terrorist organizations. In practical terms, of course, both legislated content control and private initiatives require the participation of private enterprises, particularly Internet service providers and search engine companies, and pressure has increasingly been brought to bear on such firms, both by nation states and private groups and individuals, to regulate terrorism-related content. The availability of appropriate control technologies is also considered.

Three approaches to content policy

Content policy is generally approached from one of three standpoints: human rights (freedom of expression and right to communicate), government (legislated content control) and technology (tools for content control).

Freedom of expression and the right to seek, receive and impart information is a fundamental human right, according to Article 19 of the United Nations Universal Declaration of Human Rights (1948). On the other hand, the declaration also recognizes that freedom of expression is counterbalanced by the right of states to limit freedom of expression for the sake of morality, public order and general welfare (Article 29). Thus, both the discussion and the implementation of Article 19 must be put in the context of establishing a proper balance between these two concerns. This ambiguous international regime opens many possibilities for different interpretations of norms relating to speech, and ultimately for diverging implementation.

Content control is very much bound up with free speech and concerns regarding restrictions on freedom of expression. Controls on Internet-based speech are especially contentious in the US context, where the First Amendment guarantees broad freedom of expression, even the right to publish hate speech and similar material. Achieving a proper balance between content control and freedom of expression has therefore proven to be a considerable challenge, and much of the recent Internet governance debate, including court cases and legislation, has been concerned with finding this balance. Whereas the US Congress has inclined toward stricter content control, particularly in the wake of 11 September 2001, the US Supreme Court has sought to uphold First Amendment protections. This commitment to freedom of expression is what largely shapes the US position in the international debate on Internet governance. So while the United States has signed up to the Cybercrime Convention, it is constitutionally barred from signing the Additional Protocol to the convention, which deals with the criminalization of acts of a racist and xenophobic nature committed through computer systems.[8] In other words, while the Additional Protocol is now available to European Union (EU) governments and other signatories, adding to other hate crimes statutes under which they may prosecute terrorist groups and their supporters who publish hate material online, the same legal options are not available to US authorities.

It is for this reason that many terrorist groups' sites are hosted in the United States. For example, a Connecticut-based ISP was at one time providing colocation and virtual hosting services for a Hamas site in data centres located in Connecticut and Chicago. While sites such as those maintained by Hamas have been subject to more intense scrutiny following 11 September 2001, similar web sites had already been the subject of debate beforehand. In 1997, controversy erupted when it was revealed that the State University of New York (SUNY) at Binghamton was hosting the web site of the Revolutionary Armed Forces of Colombia (FARC), and that a Túpac Amaru Revolutionary Movement solidarity site was operating out of the University of California, San Diego (UCSD). SUNY officials promptly shut down the FARC site. In San Diego, officials decided in favour of free speech, and the Túpac Amaru site remained in operation on UCSD's servers for some years.

States have access to myriad technologies with which they can limit and constrain how dissidents are able to use the Internet.

Constitutional guarantees notwithstanding, states are not technologically impotent when faced with political violence groups seeking to use the Internet to disseminate information. Rather, states have access to myriad technologies with which they can limit and constrain how dissidents are able to use the Internet. The successful use of the Internet for recruitment and other types of political action is based on the assumption that both users and audiences have access to the messages communicated via the Internet. States can therefore constrain the effectiveness of these cyber-based strategies by limiting user and audience access to Internet technologies, either by actively censoring Internet content or by controlling the Internet infrastructure, or by some combination of the two. The common element for governmental filtering is generally an index of web sites that citizens are blocked from accessing. If a web site appears on this list, access will not be granted. Technically speaking, the filtering typically utilizes router-based Internet Protocol (IP) blocking, proxy servers and DNS redirection. Filtering of content is carried out in many countries: in addition to those countries, such as China, Saudi Arabia and Singapore, which are usually associated with such practices, other countries increasingly practise censorship too. For example, Australia has a filtering system for specific national pages, while the German state of North Rhine-Westphalia requires ISPs to filter access mainly, but not solely, to neo-Nazi sites.

Three types of content

Discussions about content also usually focus on three types. The first type consists of content where a global consensus regarding its control exists. Control of the dissemination of child pornography online is the area in which the greatest amount of consensus currently exists. While incitement or organization of terrorist acts are prohibited by international law (*jus cogens*)—that is, a general consensus about the need to remove this content from the Internet has been established—disputes still arise. This is because there is no globally accepted definition of terrorism, which makes it difficult, not to say impossible, to come to any agreement as to what exactly might constitute support for terrorism in any given instance.

In terms of controls, the second type of content generally under discussion is that which might be sensitive for particular countries, regions or ethnic groups due to their particular religious or cultural values. There can be little doubt that globalized, high-volume and more intensive communication challenges cultural and religious values. In fact, most Internet court cases are concerned with this type of content. Germany has highly developed jurisprudence in this area, having tried many cases against those responsible for web sites hosting Nazi materials. In France, a court requested that Yahoo.com (USA) prohibit French citizens from accessing parts of a web site selling Nazi memorabilia. And most content control in Asia and the Middle East is officially justified as the protection of specific cultural values. This usually includes blocking access to pornographic and gambling sites, but also those of a radical political nature.

This leaves the third type of content that is often discussed, which consists of politically and ideologically sensitive materials. In essence, this involves Internet censorship. There is a dilemma here between the "real" and "cyber" worlds. Existing rules about speech, promulgated for application in the real world, *can* be implemented on the Internet. This is probably best illustrated within the European context where, for example, the EU Council Framework Decision on Combating Racism and Xenophobia may be summed up by the observation that what is illegal offline is illegal online.[9] However, one of the arguments put forward by those who believe that the Internet requires specific legislation tailored to its specific characteristics is that quantity (i.e. intensity of communication, number of messages, etc.) makes a qualitative difference. According to this view, the problem of hate and terrorism-related speech is not that no regulation against it has been enacted, but that the share and spread of the Internet render cyber-based hate and terrorism different kinds of legal problems than their real-world equivalents. In particular, more individuals are exposed to this type of speech and it is difficult to enforce existing rules. Therefore, the difference that the Internet brings relates mainly to problems of enforcing the rules, rather than the rules themselves.

The contemporary legislative landscape

The legal vacuum in the field of content policy that characterized early Internet use provided national governments with high levels of discretion in content control. National regulation may provide better protection for human rights and resolve the sometimes ambiguous roles of ISPs, enforcement agencies, and other players, but such laws may also prove highly divisive. In recent years, many countries have for the first time introduced Internet content policy legislation. Some of this legislation was introduced as a result of the boom in Internet use and the perceived need to protect the interests of user-citizens; however, a large amount of content policy was also hastily promulgated after 11 September 2001 on the basis of perceived risks to national security. Civil libertarians and others point to the knee-jerk nature and dubious efficacy of some such policies.

The US position

In the immediate aftermath of the events of 11 September, the Federal Bureau of Investigation (FBI) was involved in the official closure of hundreds, if not thousands, of US-based Internet sites. For instance, several radical Internet radio shows, including IRA Radio, Al Lewis Live and Our Americas, were pulled by an Indiana ISP in late September 2001 after the FBI contacted them and advised that their assets could be seized for promoting terrorism.[10] However, because these and many of the other sites that were closed did not directly incite violence or raise money, they were not contravening US law and many were up and running again relatively shortly after they had been shut down.

Of all the legislation promulgated in the wake of 11 September, the most relevant in terms of Internet governance is the USA PATRIOT Act of 2001, which makes it illegal to advise or assist terrorists, including via an Internet site.[11] The case of Babar Ahmad is an interesting one in this regard. Ahmad, a British citizen, was the publisher of two prominent *jihadi* web sites, azzam.com and qoqaz.net, which were hosted in the United States and through which he is accused of raising money for Islamic militants in Chechnya and elsewhere. The UK government has agreed to a US extradition request and Ahmad is to be tried in the United States on charges relating to his use of the Internet for terrorism-related purposes, which fall under the heading of "conspiracy to provide material support to terrorists".[12] This includes not just the solicitation of financial support referred to above, but also, according to an affidavit filed in the US District Court in Connecticut in 2004, urging all Muslims to "use every means at their disposal to undertake military and physical training for jihad" and providing "explicit instructions" about how to raise funds and funnel these to violent fundamentalist organizations through front organizations operating as charities.[13]

Similar charges to those pending against Ahmad have been brought against other US residents. However, due to the high levels of speech protection in the United States, at least two defendants have so far been tried and freed without charge on the basis of similar complaints: these are Sami Omas al-Hussayen, a PhD candidate in computer science at the University of Idaho who established and maintained a radical web site, and Sami Amin al-Arian, a professor at the University of South Florida who was tried on charges relating to, among other things, his utilization of the Internet to publish and catalogue acts of violence committed by Palestinian Islamic Jihad. Babar Ahmad's trial will serve as yet another test of the USA PATRIOT Act. Clearly, Ahmad's case will be one to watch in terms of its impact on terrorism-related Internet-based speech in the United States.

The UK position

The July 2005 London bombings provided the spur for the British government to act against terrorist web sites operating out of the United Kingdom. In the immediate aftermath of the attacks, the then Home Secretary (Interior Minister) Charles Clarke indicated in a parliamentary speech that he would be seeking to extend the state's powers "to deal with those who foment terrorism, or seek to provoke others to commit terrorist acts".[14] In his speech, Clarke noted specifically that "running websites or writing articles that are intended to foment or provoke terrorism" were activities that would fall within the ambit of these new powers.[15] The prevention of terrorism bill 2005 narrowly avoided defeat in Westminster in October 2005; opposition centred on two key measures: new police powers to detain suspects for up to 90 days without charge and a proposed offence of "encouragement or glorification of terrorism". With regard to the "glorification of terrorism", such a measure would clearly criminalize the establishment, maintenance and hosting of many web sites currently operational within the United Kingdom.

The major criticism, of course, is that the latter clause may serve to stifle legitimate political speech. Several other measures included in the bill that may also impact upon terrorist Internet use in the United Kingdom, such as the outlawing of acts preparatory to terrorism and the giving or receiving of terrorism training, went largely uncontested in parliamentary debates. In the event, the government was defeated on the issue of detention. However, the remainder of the bill's provisions went into force and became the Terrorism Act 2006.[16] What impact the new legislation will have on terrorism-related materials produced by or disseminated to UK citizens via the Internet is unknown at the time of writing.

International initiatives

At the international level, the main content control initiatives have been undertaken by European countries that already have strong legislation in the area of hate speech, and by European regional institutions trying to impose those same rules in cyberspace. The key international legal instrument addressing the issue of content is the Council of Europe's Additional Protocol to the Cybercrime Convention. The protocol specifies various types of hate speech that should be prohibited on the Internet, including racist and xenophobic materials, justification of genocide and crimes against humanity. The Organization for Security and Co-operation in Europe (OSCE) is active in this field also. In June 2003, the OSCE conference on The Freedom of the Media and the Internet adopted the Amsterdam Recommendations on Freedom of the Media and the Internet. The recommendations promote freedom of expression and attempt to reduce censorship on the Internet. In June 2004, the OSCE organized a meeting on The Relationship between Racist, Xenophobic and Anti-Semitic Propaganda on the Internet and Hate Crimes. The focus of this event was on the potential misuses of the Internet and freedom of expression. These OSCE events provided a wide range of academic and policy views of these two aspects of content control, though no new rules were instituted as a result of these discussions.

The key international legal instrument addressing the issue of content is the Council of Europe's Additional Protocol to the Cybercrime Convention.

On a more practical level, in May 2007 EU ambassadors agreed that the European Police Office's (Europol) newly established high-security online portal known as *Check the Web* will need to be further strengthened to combat terrorism. The web site allows the 27 EU states to pool data on Islamist propaganda and Internet chatter and provides details on the experts monitoring the web in EU countries.

Check the Web is accessible only to law enforcement and experts, but the EU Safer Internet Action Plan has resulted in the establishment of a European network of hotlines, known as Inhope, for the reporting of illegal content by the general public. At the present time, the major type of illegal content focused upon is child pornography and paedophilia. However, there is nothing stopping national governments or EU bodies from instituting a similar reporting system for terrorism-related content.

The role of private actors

Legislating for terrorism-related content on the Internet is clearly the domain of governments. However, because of the nature of the Internet, private companies and groups are never far from the frontline. In this section, the focus is on actors other than states and their contributions to the effort to eradicate terrorism-related materials from the Internet. Two groups in particular are focused on: Internet search companies and hacktivists.

Geolocation software

In analyses of Internet governance, one of the key arguments frequently advanced was that the decentralized nature of the Internet made attempts at censorship redundant. Today, this is in many respects untrue: the Internet includes many techniques and technologies that can provide effective control. Having said this, from a technology standpoint, control mechanisms can also be bypassed. In states with government-directed content control, technically savvy users have found ways around such controls.

It is still difficult to identify exactly who is behind any given computer screen, but it is fairly straightforward to identify through which Internet service provider the Internet was accessed. Worldwide, the latest national legislation requires ISPs to identify their users and, if requested, to provide necessary information about them to authorities. Numerous governments have also announced plans to monitor more closely those who access the Internet in public places, particularly Internet cafés. Increased surveillance of the latter is now taking place in India, Italy, Thailand and a host of other countries; the explanation generally offered is "national security". The more the Internet is anchored in space, the less unique its governance will be. For example, with the possibility to geographically locate Internet users and transactions, the complex question of jurisdiction on the Internet can be solved more easily through existing laws.

One technical solution is geolocation software, which identifies the location of a computer and filters access to particular Internet content according to the national origin of the computer. The Yahoo! case was important in this respect, since the group of experts involved indicated that in 90% of cases, Yahoo! would be able to determine whether sections of one of its web sites hosting Nazi memorabilia were being accessed from France. This technological assessment helped the court to come to a final decision. Geolocation software companies claim that they can currently identify the home country without error and the accessing city in about 85% of cases, especially if it is a large city. Such software can therefore help Internet content providers filter access according to nationality and thus avoid court cases in foreign jurisdictions.

Content control by search engines

There are significant differences between the availability and the accessibility of online materials: the fact that particular web-based content is available on the Internet does not mean that it can be easily accessed by large numbers of users. The bridge between the end-user and web content is usually a search engine. Therefore, if a particular web site cannot be found on Google or another major search engine, its visibility is seriously diminished. On German and French versions of Google, it is not possible to search for and find web sites with Nazi materials, for example. This indicates a certain level of self-censorship on the part of Google in order to avoid possible court cases. In terms of terrorist web sites, many Internet companies voluntarily purged sites perceived as terrorist after 11 September 2001. For example, Yahoo! pulled dozens of sites in the Jihad Webring, a coalition of 55 *jihad*-related sites, while Lycos Europe established a 20-person team to monitor its web sites for illegal activity and to remove terrorism-related content. However, such policies of compliance can be viewed as political in character and have thus come under fire, particularly from free-speech advocates.

Hackers and hacktivists

The events of 11 September 2001 acted as the spur for many private groups and individuals to take to the Internet in search of "terrorist" web sites to disrupt. Computer hackers were particularly well placed to engage in this sort of activity. In the immediate aftermath of the attacks, for example, a group calling itself The Dispatchers proclaimed that it would destroy web servers and Internet access in Afghanistan and also target nations that support terrorism. The group proceeded to deface hundreds of web sites and launch Distributed Denial of Service (DDoS) attacks against targets ranging from the Iranian Ministry of the Interior to the Presidential Palace of Afghanistan. Not all hacking groups were supportive of the so-called hacking war. On 14 September 2001, the Chaos Computer Club, an organization of German hackers, called for an end to the protests and for all hackers to cease vigilante actions. In the weeks following the attacks, web page defacements were well publicized, but the overall number and sophistication of these remained rather low. One possible reason for the non-escalation of attacks could be that many hackers were wary of being negatively associated with the terrorist attacks of 11 September and curbed their activities.

It has never been all plain sailing for terrorist users of the Internet, even prior to September 2001. Home pages have been subject to intermittent DDoS and other hack attacks, and there have also been strikes against their ISPs that have resulted in more permanent difficulties. In 1997, for example, an e-mail bombing was conducted against the Institute for Global Communications (IGC), a San Francisco-based ISP, hosting the web pages of the *Euskal Herria* or *Basque Country Journal,* a publication edited by supporters of the Basque group Fatherland and Liberty (ETA). The attacks against IGC began after ETA's assassination of a popular town councillor in northern Spain. The protesters wanted the site pulled from the Internet and IGC eventually removed it from its servers, but not before archiving a copy of the site, enabling others to put up mirrors: mirror sites appeared on half a dozen servers on three continents. Despite this, the protesters' e-mail campaign raised fears of a new era of censorship imposed by direct action from anonymous hacktivists.

Since September 2001 a number of more formal web-based organizations have been established to monitor terrorist web sites. One of the most well-known of such sites is Internet Haganah, self-described as "an Internet counterinsurgency". Also prominent is the Washington, DC-based Search for International Terrorist Entities (SITE), which, like Internet Haganah, focuses on Islamist terror groups. Clients of SITE's fee-based intelligence service are said to include the FBI, the Office of Homeland Security and various media organizations. But what are the goals of these private organizations? SITE is engaged in the collection (and sale) of open source intelligence—co-founder and director Rita Katz has commented: "It is actually to our benefit to have some of these terror sites up and running by US companies. If the servers are in the US, this is to our advantage when it comes to monitoring activities."[17] Aaron Weisburd, who runs Internet Haganah, says his goal is to keep the extremists moving from address to address: "The object isn't to silence them—the object is to keep them moving, keep them talking, force them to make mistakes, so we can gather as much information about them as we can, each step of the way".[18] Weisburd's *modus operandi* is first to research a site, then make a "whois" inquiry. If there is evidence of extremism, he contacts the hosting company and urges the host to remove the site from its servers. If successful, Internet Haganah may purchase the domain name so the address can never be used again. Since its inception in 2003, Internet Haganah has taken credit for or claims to have assisted in the shutdown of more than 600 sites it alleges were linked to terrorism.

Conclusion: where do we go from here?

While the potential of a "digital 9/11" is not great in the near future, the Internet has come of age since 2001. Both terrorism and the Internet are significant global phenomena, reflecting and shaping various aspects of world politics. Due to its global reach and rich multilingual context, the Internet has the potential to influence in manifold ways many different types of political and social relations. Unlike the traditional mass media, the Internet's open architecture means that efforts by governments to regulate Internet activities are restricted, and this has provided users with immense freedom and space to shape the Internet in their own likeness. Included within this cohort are terrorists who increasingly employ new media to pursue their goals. The terrorists of today, like those of yesteryear, are keen to exploit the traditional mass media while also recognizing the value of more direct communication channels.

As far back as 1982, Alex Schmid and Janny De Graaf conceded that:

> If terrorists want to send a message, they should be offered the opportunity to do so without them having to bomb and kill. Words are cheaper than lives. The public will not be instilled with terror if they see a terrorist speak; they are afraid if they see his victims and not himself […] If the terrorists believe that they have a case, they will be eager to present it to the public. Democratic societies should not be afraid of this.[19]

Not everybody is in agreement with this position, however. Over time, both state and non-state actors have endeavoured to curb the availability of terrorism-related materials online with varying degrees of success. Authoritarian governments have met with some success by deploying technologies that constrain their citizens' ability to access certain sites. There are fewer options for restriction available to democratic governments, however, and although recently more restrictive legislation has been promulgated in a number of jurisdictions, it is not yet clear that it will be any more successful than previous attempts at controlling, for example, cyber-hate. In terms of terrorist web sites and their removal, private initiatives instituted by a range of substate actors in conjunction with ISPs have been much more successful. But the activities of individual hacktivists raise a number of important issues relating to limits on speech and who can and should institute these limits. The capacity of private political and economic actors to bypass the democratic process and to have materials they find politically objectionable erased from the Internet is a matter for concern. Such endeavours may, in fact, cause us to think again about legislation, not just in terms of putting controls in place—perhaps, for example, outlawing the posting and dissemination of beheading videos—but also writing into law more robust protections for radical political speech.

Notes

1. See WSIS Plan of Action, World Summit on the Information Society, Geneva, 12 December 2003, document WSIS-03/GENEVA/DOC/5-E, at <www.itu.int/wsis/docs/geneva/official/poa.html>, paragraph 13b.
2. Eduardo Gelbstein and Jovan Kurbalija, 2005, *Internet Governance: Issues, Actors and Divides,* Geneva, DiploFoundation and Global Knowledge Partnership, at <www.diplomacy.edu/isl/ig>, pp. 10–12.
3. Hans Klein, 2002, "ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy", *The Information Society,* vol. 18, no. 3, pp. 194–195.
4. *Report from the Working Group on Internet Governance,* document WSIS-II/PC-3/DOC/5-E, 3 August 2005, paragraph 10.
5. Paul Eedle, "Al Qaeda's Super-Weapon: The Internet", paper presented at the conference "Al-Qaeda 2.0: Transnational Terrorism After 9/11", Washington, DC, 1–2 December 2004.

6. The video is entitled "Abu Musab al-Zarqawi Shown Slaughtering an American", and Central Intelligence Agency officials have since stated that it assesses with "high probability" that it is al-Zarqawi that carried out the beheading ("Jamaat al-Tawhid wa'l-Jihad / Unity and Jihad Group", *Global Security.org,* at <www.globalsecurity.org/military/world/para/zarqawi.htm>, and "'Zarqawi' beheaded US man in Iraq", *BBC News,* 13 May 2004, at <news.bbc.co.uk/2/hi/middle_east/3712421.stm>).
7. Eedle, op. cit.
8. Additional Protocol to the Convention on Cybercrime, signed at Strasbourg, 28 January 2003, at <conventions.coe.int/Treaty/EN/Treaties/Html/189.htm>.
9. Proposal for a Council Framework Decision on Combating Racism and Xenophobia, Official Journal of the European Communities 2002/C 75/E17, 26 March 2002.
10. Al Lewis Live can still be heard on Pacifica Radio in the United States. The IRA Radio site was allowed back online in March 2002 at <www.iraradio.com>. However, it appears to have closed down again some time after February 2003. The other sites mentioned remain offline.
11. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).
12. *United States of America* v. *Babar Ahmad and Azzam Publications,* Indictment, United States District Court, District of Connecticut, at <www.usdoj.gov/usao/ct/Documents/AHMAD%20indictment.pdf>.
13. "British Man Arrested on Several Terrorism-related Charges", Press Release, United States Attorney's Office District of Connecticut, 6 August 2004, at <www.usdoj.gov/usao/ct/Press2004/20040806.html>.
14. Charles Clarke, in House of Commons Debates, *Hansard,* vol. 436, 20 July 2005, Column 1255.
15. Ibid.
16. The full text of the Act may be viewed at the web site of the UK's Office of Public Sector Information <www.opsi.gov.uk/acts/acts2006/20060011.htm>. See in particular Part 1, Section 3, "Application of ss. 1 and 2 to Internet activity, etc".
17. Quoted in John Lasker, "Watchdogs Sniff Out Terror Sites", *Wired News,* 25 February 2005.
18. Ibid.; see also Gary Bunt, 2003, *Islam in the Digital Age: E-Jihad, Online Fatwas and Cyber Islamic Environments,* London, Pluto Press, pp. 24 and 93.
19. Alex P. Schmid and Janny De Graaf, 1982, *Violence as Communication: Insurgent Terrorism and the Western News Media,* London, Sage, p. 170.

Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law

Sergei Komov, Sergei Korotkov and Igor Dylevski

Nearly a decade has passed since the Russian Federation launched its initiative within the United Nations to address the issue of international information security (IIS). This complex issue is closely related to a number of fundamental principles of international law, including the prohibition of wars of aggression, the non-use of force or threat of force, and non-interference in another state's internal affairs.

The shocks suffered by mankind as a result of two World Wars played a special role in the international community's transition to civilized means of resolving international problems. Following the First World War, the term "war of aggression" was referred to as an international crime for the first time in a number of international instruments. The Kellogg-Briand Pact was the first multilateral treaty to set forth in international law the principle prohibiting wars of aggression.[1] The treaty proclaimed that war should be renounced as an instrument of national policy to settle international disputes and that all disputes should be settled peacefully.

After the Second World War, the prohibition on wars of aggression further evolved into a comprehensive principle of the non-use of force or threat of force in international relations. The principle of non-interference in the internal affairs of other states has also developed as an imperative principle of international law.

The Soviet Union played a pivotal role in establishing the principle of prohibition of wars of aggression and its successive transformation into the principles of non-use of force and non-threat of force. In particular, in 1933 the Soviet Union tabled a draft definition of aggression at the General Commission of the International Conference on Disarmament; although this definition was not adopted, it laid the foundation for many international instruments developed following the Second World War. In 1953, the Soviet delegation submitted a new draft definition of aggression to the Special Committee established by the UN General Assembly.[2]

In hindsight, an important advantage of the 1953 draft definition was its comprehensive nature, addressing four major types of aggression: direct (military), indirect, economic and ideological.[3] In particular, it proposed to recognize that a state had committed indirect aggression if it was the first to:

a) encourage subversive activities against another state (through terrorist attack, diversion, etc.);

b) contribute to inciting civil war in the other state; or

c) contribute to a coup d'état in another state or a policy change that would favour an aggressor.

Sergei Komov, Sergei Korotkov and Igor Dylevski are experts at the Ministry of Defence of the Russian Federation. They took part in the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2004–2005) and the relevant Group of Experts of the Shanghai Cooperation Organization Member Countries (2006–2007).

The following were considered as acts of ideological aggression:

a) encouraging war propaganda;

b) encouraging propaganda promoting the use of nuclear, bacteriological, chemical and other weapons of mass destruction; and

c) supporting propaganda of Fascist or Nazi ideas of race and national exclusiveness, hate and depreciation towards other nations.

The draft definition also specified that the acts of aggression listed were not exhaustive, and that the UN Security Council could also consider other acts as aggression.

As a result of significant differences among the members of the Special Committee at its VII session, a draft definition of aggression was ultimately agreed upon that included only the military component. In December 1974, this definition was adopted by the UN General Assembly.[4] That resolution sets forth a general definition of aggression (Article 1), specifies the main prima facie evidence of an act of aggression (Article 2) and lists major acts of aggression (Article 3). It also stresses that the list is not exhaustive and that the Security Council may determine that other acts constitute aggression under the provisions of the Charter (Article 4). In addition, it stipulates that "no consideration of whatever nature, whether political, economic, military or otherwise, may serve as a justification for aggression" (Article 5).

A cornerstone in the transformation of the principle concerning prohibition of wars of aggression into a more fundamental principle of non-use of force or threat of force was the UN Charter, which states that "all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations" (Article 2.4).

Other international instruments confirmed and further developed this principle, turning it into an imperative norm of international law. In particular, the 1970 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations[5] states that:

> A war of aggression constitutes a crime against the peace, for which there is responsibility under international law.
>
> In accordance with the purposes and principles of the United Nations, States have the duty to refrain from propaganda for wars of aggression.
>
> …
>
> Every State has the duty to refrain from any forcible action which deprives peoples referred to in the elaboration of the principle of equal rights and self-determination of their right to self-determination and freedom and independence.[6]

Moreover, in this declaration the principle of non-use of force or threat of force is connected with the principle of non-intervention in the internal affairs of another state, affirming that:

> … armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.
>
> No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed

> towards the violent overthrow of the régime of another State, or interfere in civil strife in another State.
>
> The use of force to deprive peoples of their national identity constitutes a violation of their inalienable rights and of the principle of non-intervention.[7]

On the threshold of the third millennium many experts came to understand the necessity of legally prohibiting the use not only of the force of arms, but also of any other violence that constitutes an unlawful use of force for the purpose of aggression or intervention in the internal affairs of another state. Such a broad interpretation of the notion of "force" covers both economic and energy coercion, as well as other forms of violence in international relations.

Today, all societies are information dependent. The conduct of so-called "information operations" is therefore one of the potentially most damaging forms of force. These operations primarily aim at disrupting the functioning of the enemy's key military, industrial and administrative facilities and critical systems, and at manipulating information and exerting psychological influences on another state's political and military authorities, troops and civil population using, in the first place, information and communication technologies (ICTs).

ICTs make it possible to carry out electronic and computer attacks that are fundamentally different from traditional physical attacks. The use of electronic means takes warfare from the physical dimension to the virtual one. Today, a state can be attacked without its territory ever being physically invaded. The damage from such an attack may take different forms, for instance, technical failure of critical industrial, economic, energy and transport facilities, as well as financial collapse and large-scale crisis. Additionally, significant non-material damage could be inflicted as a result of disruption of civil order and military authority, including demoralization or disorientation of the population or mass panic.

Today, a state can be attacked without its territory ever being physically invaded.

The United States is considered to be the world leader in information operations, and intends to continue increasing its already existing powerful intelligence resources, and electronic warfare and psychological operations capacities.[8] For example, the US Air Force has announced the creation the Air Force Cyber Command, which will become operational this year. Within the US Strategic Command (STRATCOM), the Joint Functional Component Command for Network Warfare is the leading unit for information operations.[9]

The potential of information operations is evident to military experts. However, information operations are a relatively new phenomenon in international relations. For numerous general and political reasons, members of the international community have yet to undertake a proper international legal evaluation of the issue.

It comes as no surprise that the United States is averse to attempts to discuss military aspects of the problem of international information security. A key participant in most major military actions of the past fifty years, it traditionally does not recognize some important, generally accepted provisions regulating the use of force in international relations and intervention in the internal affairs of other states. This is not a new development: as early as the mid-twentieth century during the discussion of the ideological component of the Soviet definition of the notion "aggression" an American representative voiced disagreement, stating that what may be considered propaganda in one country may be just the statement of a free press in another.[10] More recently, in the context of developing the Rome Statute of the International Criminal Court, the US delegation raised an objection to the 1974 definition of aggression, an action which some have interpreted as hedging against the possibility that aggression be considered—and thus responsibility for such—an international crime.[11]

For reasons such as these, in 2005 the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[12] was unable to reach consensus on the adoption of its final substantive report. Thus, the opportunity to comprehensively address the problem of IIS in an international expert-level forum was postponed until 2009, when a new Group of Governmental Experts is scheduled to begin work.

As to the legal aspect of the problem, the way forward is, first of all, the application of universally accepted principles of international law in inter-state relations to the field of planning and execution of information operations. This will naturally require the adaptation of these principles to the specific character of these new inter-state relations. This approach will lay the necessary international legal foundation for addressing both the problem of ensuring IIS in general, and its political and military aspects in particular. Legal aspects of other relevant fields, such as outer space law, humanitarian law, and international legal responsibility, will also need to be taken into consideration.

The application and development of key principles of international law

At present international law lacks provisions that unambiguously prohibit, allow or otherwise regulate information operations. However, such issues could be considered in the context of the application of key international legal principles. In particular, the aforementioned 1974 definition of aggression[13] states that not only military violence but also other acts of aggression as defined by the Security Council qualify as aggression under the UN Charter. However, this provision has yet to be utilized. Even earlier, in 1953 Iran proposed in the General Assembly that any action that indisputably serves the purpose of an armed attack or results in coercion prejudicing the independence of a state should be recognized as aggression.

Since the adoption of the UN Charter the principle of non-use of force or threat of force against the territorial integrity or political independence of another state has been applied only in its physical sense. The 1973 oil embargo led many nations to question the point of view that use of force did not include economic coercive measures, as the UN Charter prohibits the threat of force and its use in any way that is incompatible with the Purposes of the United Nations. Other states insisted that the said provision did not apply to such a manifestation of force.[14]

Ultimately, United Nations resolutions and enforcement practice do not provide a definitive answer to the question of whether an attack as part of an information campaign would be classified as aggression, use of force or threat of force. Therefore, there is a need to develop these principles to define in more detail the concepts of "aggression", "force" and "threat of force" in relation to IIS.

As for classifying "information and psychological influence" as intervention in the domestic affairs of a state, this issue could be resolved on the basis of the provisions of the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations[15] and the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty,[16] the latter of which states that "No State has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are condemned."[17]

Although these documents do not provide a clear definition of "intervention in the domestic affairs of states", they contain an open-ended list of actions that qualify as intervention. This legal platform leads us to the conclusion that almost any information operation with a psychological bias, implemented in peacetime with respect to another state, would qualify as intervention in its domestic affairs. Even good intentions, such as the advancement of democracy, **cannot** justify such operations.

The 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States further developed the principle of non-intervention in the domestic affairs of states. These rights and obligations of states include:

- "The right of States and peoples to have free access to information and to develop fully, without interference, their system of information and mass media and to use their information media in order to promote their political, social, economic and cultural interests and aspirations, based, *inter alia,* on the relevant articles of the Universal Declaration of Human Rights and the principles of the new international information order";[18]
- "The duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States";[19] and
- "The right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news which can be interpreted as interference in the internal affairs of other States or as being harmful to the promotion of peace, co-operation and friendly relations among States and nations".[20]

Consequently, the dissemination of disinformation by one state against another, widely used in information operations, may be considered intervention in its domestic affairs and should entail corresponding measures of international responsibility.

International law prohibits the violation of a neutral state's territory by a belligerent's armed forces. However, belligerent states are not under obligation to refrain from using open computer networks of a neutral state. Moreover, the use of computer networks crossing the territory of a neutral state to conduct information operations could be considered as a violation of its territory. These forms of aggression can therefore be considered illegitimate acts of warfare against a neutral state. On the other hand, if a neutral state refuses to oppose the use of its networks for attacking another party, it might be targeted by the state against which an information operation is being conducted under the pretext that its networks were used.

The legality of retaliatory actions against information operations is another significant legal issue. To clarify this issue, the international community has to resolve a number of integrated problems. In particular, it is necessary to be able to identify with certainty the source of a cyber attack and to consider the issue of territorial jurisdiction.

According to international law, foreign agents cannot carry out their activities within the territory of another state without its permission. The UN International Court of Justice in the Corfu Channel Case (1949) ruled that the entry of the British Royal Navy into Albanian territorial waters without permission was seen as a manifestation of force and a violation of international law.[21] More recently, the Council of Europe has attempted to find a solution based on international law to the territorial jurisdiction issue with a view to ensuring international information security in computer networks.[22] Some experts believe that this has not been a very successful approach, believing that it entails the violation of such principles as national sovereignty and non-interference in the internal affairs of other states.

In accordance with Article 51 of the UN Charter, individual or collective self-defence against armed aggression is regarded as lawful use of force. At the same time it is not clear whether this article permits retaliatory military action against a state carrying out an information operation. In the 1986 case Nicaragua against the United States of America, the UN International Court of Justice found that states are not entitled to take military action in retaliation for acts that do not constitute military aggression.[23] Based upon this precedent, unless cyber attacks are qualified as armed aggression, the injured party will not have the legal right to respond in self-defence using conventional weapons. Yet ironically, within the current legal ambiguity surrounding IIS issues, symmetrical retaliatory measures (i.e. information attacks) could be taken with impunity. The simple legal solution to this problem requires requesting the Security Council to qualify a cyber attack as posing a threat to the peace or as an act of aggression, which would then permit an attacked state to take certain measures provided for within UN Charter.

Contemporary international law has a number of concepts to describe actions taken by one state against another as aggression, use of force or threat of force and interference in internal affairs. All of these concepts apply to both armed forces and state-backed terrorist groups. Today's interpretation of these concepts is conditioned by the historical practice of waging warfare with conventional military means. This makes it very hard to define the term "information operations" carried out by either traditional or fundamentally new means. It is easiest to qualify the concept of "interference in the internal affairs of a state", which comprises all possible means that have information and psychological effects. As to such information effects as electronic and cyber attacks, we think that it is advisable they are included within the concepts of "aggression", as well as the "use of force" or "threat of force". Moreover, a mechanism in international law already exists, via the UN Security Council, to determine a threat to the peace or an act of aggression. It is this mechanism used under the UN Charter that must establish whether an information operation has occurred and which state conducted it, as well as to determine appropriate steps to restore international peace and security and appropriate measures to prevent the further violation of these principles.

Application and development of principles in select branches of international law

Important provisions concerning the military aspects of information security are contained in documents that form the basis of such branches of international law as international telecommunications law, space law, international humanitarian law, law of international legal responsibility of states, and others.

Some actions taken as part of information operations related to electronic warfare may be covered by instruments of international telecommunications law. Thus, under the Constitution of the International Telecommunication Union (ITU), all communication stations, whatever their purpose (including military ones), must be established and operated in such a manner so as not to cause harmful interference to the radio services or communications of other Member States. Member States further agree to take the steps required to prevent the transmission or circulation of false or deceptive distress, urgency, safety or identification signals, and to collaborate in locating and identifying stations under their jurisdiction transmitting such signals.[24]

Activities carried out as part of peacetime information operations entailing consequences prohibited by the ITU Constitution may therefore be considered as violating this international agreement. However, there would be no violation if the information operation is qualified as an armed conflict or if it occurred during an armed conflict.

If satellites were to be used to conduct an information operation, *international space law* may apply. The cornerstone of international space law, the Outer Space Treaty, obliges states to carry out their space activities exclusively for peaceful purposes.[25] However, some believe that space law does not directly prohibit the use of satellites for conducting information operations. Within the Conference on Disarmament, the United States has opposed discussion of the 2002 working paper "Possible Elements for a Future International Legal Agreement on the Prevention of the Deployment of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects".[26] In the General Assembly, it has voted against resolutions on the Prevention of an Arms Race in Outer Space[27] and on Transparency and Confidence-Building Measures in Outer Space Activities,[28] stating in its Explanation of Vote that there is no arms race in outer space and "thus no arms control problem for the international community to address." Some fear that this position aims to maintain conditions allowing the use of outer space for conducting global information operations.

An essential principle of international humanitarian law (IHL) is that of humanity in armed struggle, which prohibits the use of force unless it is justified by military necessity. The principle of humanity concerns methods and means of warfare, as well as protection of victims of war. Through IHL, belligerents are limited in their means of damaging the enemy. For example, it is prohibited to employ weapons of indiscriminate effect (i.e. directed both at military objectives and civilian objects) or causing superfluous injury or unnecessary suffering.[29] Hence, to avoid indiscriminate effects, hostilities—including in the form of information operations—should be limited to military objectives, i.e. to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

During times of conflict, protection of civilian objects, including against information operations, should be ensured in two ways:

- special precautionary measures should be taken to verify that the objective to be attacked is a military one. To avoid incidental damage to civilian objects, it is important to refrain from any attack against civilian objects which may be expected to cause damage excessive in relation to the concrete military advantage anticipated;
- special protection of objects indispensable to the survival of the civilian population, works and installations that would pose great threat if damaged or destroyed (such as nuclear power plants, dams and dykes), cultural objects and those related to civil defence.

In one view, the best way to define information operations in relation to IHL is on the basis of the scale and gravity of their consequences.[30] Disorganization of the financial system of a state, man-made disasters and panic entailed by information operations may cause mass casualties among civilians. Additionally, the dual-use nature of ICTs has eliminated the distinction between many military and civilian ICT systems. In addition to military gains, information operations may therefore lead to malfunction of civilian objects. Hence, under IHL, information operations affecting such objects should be banned.

In one view, the best way to define information operations in relation to IHL is on the basis of the scale and gravity of their consequences.

International humanitarian law does not prohibit ruses of war, such as the use of camouflage, mock operations, misinformation, etc. At the same time, perfidy is prohibited. This includes: unlawful use of flag of truce, military emblems and uniform of the enemy, the United Nations and the Red Cross; or killing or capturing an adversary by resort to perfidy. However, it is very difficult to distinguish between perfidy and ruses of war in an information operation meant to manipulate the perceptions of the civilian population or military and political leaders. As no clear criteria have yet been established in international law to deal with this issue, some claim that manipulation of perception does not violate IHL. However, it should be recalled that it was the manipulation and distortion of information that justified the unleashing of two world wars in the past century, and some claim that manipulation of intelligence data misled world public opinion to legitimize recent actions in Iraq.

Finally, it should be noted that if information operations as a form of military action are covered by the existing rules of IHL, then it necessitates application of all existing agreements on laws and customs of **war with regard to such operations.**

As for the *international legal responsibility of states* for internationally wrongful acts (in case of breach of an international obligation by a state), this is well established in contemporary international law, specifically regarding the threat or use of force.

Crimes against peace, war crimes and crimes against humanity were for the first time qualified as gravest international crimes under the charters of the international military tribunals at Nürnberg and Tokyo. A 1946 UN General Assembly resolution[31] recognized the principles contained in the Charter of the Nürnberg Tribunal as principles of international law, i.e. rules establishing the responsibility of states and criminal responsibility of individuals for the commission of international crimes. These principles are universally recognized.

We believe that the foundations for a state's liability for internationally wrongful acts in connection with information operations are as follows:

- dissemination of information prohibited by international law, including war propaganda and advocacy of the use of force, propaganda of violence, provocative information, etc.;
- dissemination of information specifically intended to produce psychological and/or ideological effects on the population or on certain individuals (false information, information fomenting religious discord and other enmity, etc.);
- cyber attacks on information systems of the state's critical infrastructure and attacks on other infrastructure, when such attacks result in substantial economic damage; and
- radio jamming, transmitting or propagating false or deceptive distress, emergency, safety or identification signals, etc.

Depending on the gravity of their consequences, such acts could be qualified as international crimes, i.e. the gravest of offences involving severe measures of international responsibility.

Given the danger of information operations, for example against critical infrastructure facilities, it seems possible in principle to raise the issue of controls on manufacturing and proliferation of means of information warfare, sometimes referred to by the umbrella term "information weapons". Imposing export controls on special-purpose technology might be a means of ensuring control of such weapons. However, some elements such as expertise and widely available technologies are currently not subject to export controls. Thus, in order to create a comprehensive international legal information weapons control system, we should draw on the experience of designing and enforcing regimes and procedures for control established by international law in relation to other types of weapons, while taking into account the specific characteristics of information weapons.

Conclusion

In the last century, when chemical, biological and, finally, nuclear weapons were created, we were unable to develop international instruments on nuclear disarmament and instruments prohibiting biological and chemical weapons were adopted only belatedly. As for nuclear weapons, the international community has yet to agree on their ban.

Today, a completely new military and political threat is emerging. The international community should not permit this situation to happen again with regard to measures to counter the threat of proliferation of information weapons and to suppress the unpunished conduct of information operations. To this end, the international community should, as a matter of priority, overcome its apathy toward continued regular violations of universally recognized principles of international law and then collectively build a reliable international legal barrier to the emerging threat of information aggression.

Notes

1. Treaty for Renunciation of War as an Instrument of National Policy, signed in Paris on 27 August 1928.
2. UN document A/AC.66/L.2/Rev.1, 14 September 1953.
3. K.A. Baginyan, "Агрессия – тягчайшее международное преступление. К вопросу об определении агрессии" [Aggression as a Major International Offence. On the Definition Aggression], *Sovetskoe Gosudarstvo i Pravo,* vol. 1, 1955.

4. General Assembly, Definition of Aggression, UN resolution 3314 (XXIX), 14 December 1974.
5. General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, UN resolution 2625 (XXV), 24 October 1970, annex.
6. General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, UN resolution 2625 (XXV), 24 October 1970, annex.
7. Ibid.
8. United States Department of Defense Directive (DODD) S-3600.1, Information Operations, October 2001; DOD Information Operations Roadmap, 30 October 2003; FM 3-13 Information Operations: Doctrine, Tactics, Techniques and Procedures, 28 November 2003, SS FM 100-6; Joint Pub 3-13 Information Operations, 13 February 2006.
9. "A Special Subdivision for Neutralizing Foreign Media Created in the USA", *NEWSru.com,* 23 November 2005.
10. K.A. Baginyan, "Багинян К.А. Агрессия – тягчайшее международное преступление. К вопросу об определении агрессии." [Aggression as a Major International Offence. On the Definition Aggression], *Sovetskoe Gosudarstvo i Pravo*, vol. 1, 1955.
11. V.A. Kartashkin (ed.), *Human Rights and Armed Conflicts,* Norma Infra, Moscow, 2001, p. 137.
12. Established in accordance with the decision of the General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, UN document A/RES/56/19, 7 January 2002.
13. General Assembly, Definition of Aggression, UN resolution 3314 (XXIX), 14 December 1974.
14. K.A. Baginyan, "Ягчайшее международное преступление. К вопросу об определении агрессии" [Aggression as a Major International Offence. On the Definition Aggression], *Sovetskoe Gosudarstvo i Pravo,* vol. 1, 1955.
15. General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, UN resolution 2625 (XXV), 24 October 1970, annex.
16. General Assembly, Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, UN resolution 2131 (XX), 21 December 1965.
17. Ibid., paragraph 1.
18. General Assembly, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, UN document A/RES/36/103, 9 December 1981, §I(c).
19. Ibid., §II(j).
20. Ibid., §III(d).
21. The Corfu Channel Case. Consideration on the merits. Decision of April 9, 1949, ICJ Reports, 1949, pp. 34–35.
22. Convention on Cybercrime (ETS No. 185), signed in Budapest on 23 November 2001.
23. The case on military and paramilitary activities in and against Nicaragua (Nicaragua against the United States of America). Decision of 27 June 1986, ICJ Reports, 1986, paragraphs 195, 232.
24. The Constitution of the International Telecommunication Union (adopted in Geneva on 22 December 1992), Articles 45, 47, 48.
25. The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (signed on 27 January 1967).
26. Permanent Representatives of China and the Russian Federation, *Possible Elements for a Future International Legal Agreement on the Prevention of the Deployment of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects,* Conference on Disarmament document CD/1679, 28 June 2002.
27. General Assembly, Prevention of an Arms Race in Outer Space, UN document A/RES/61/58, 3 January 2007.
28. General Assembly, Transparency and Confidence-Building Measures in Outer Space Activities, UN document A/RES/61/75, 18 December 2006.
29. Additional Protocol I to the Geneva Conventions (adopted on 12 August 1949), Article 35 paragraph 2, Article 52 paragraph 2, Article 57.
30. Кубышкин А.В., Международно-правовые проблемы обеспечения информационной безопасности государства [The International Legal Problem of Ensuring Information Security of a State], Doctoral Thesis, Moscow State Law Academy, 2002.
31. General Assembly, Affirmation of the Principles of International Law Recognized by the Charter of the Nürnberg Tribunal, UN resolution 95 (I), 11 December 1946.

Harnessing the perils in cyberspace: who is in charge?

Henning Wegener

There is now a common and growing awareness among individuals, politicians and academic observers that the rapid progress and introduction of new technologies, along with their tremendous benefits, entail major risks, often of a global dimension. We are living in a "world risk society", which is being analysed on an increasingly informed basis and displays alarming features.[1] In a new way, and while we take pride in our technological achievements, the world has become a very dangerous place.

Fragility of the cyberworld

One major risk factor is the vulnerability of the information and communication technology (ICT) systems that pervade all aspects of human endeavour and grow at an exponential pace. They have ushered in a new era of opportunity in terms of wealth creation, government efficiency, human development and global business opportunities, and have led to the emergence of a new type of knowledge society through vast new options for knowledge acquisition and sharing. Information technology (IT) has become the critical raw material of all societal activity. Computing capabilities, telecommunications, the Internet and the capabilities of broadband data transportation networks negate the relevance of frontiers and distances, and increasingly enable the vision of a global society with a new division of labour and shared benefits, and more inclusive and integrated national societies.

However, the primary cause of vulnerability is the sheer increase in volume of ICT devices worldwide. There are now more than one billion computers and tens of billions of other—equally vulnerable—processors and microprocessors in operation, the latter as embedded systems that invisibly govern vital controlling, monitoring and steering equipment. Then, the impending migration of most telephones, computing devices and sensors, both fixed and mobile, to the Internet Protocol (IP) mode will multiply the number of vulnerable devices further. The telecommunications and IT world will increasingly converge and commingle in next-generation networks, enabling ubiquitous and invisible computing in an "ambient intelligent" environment. All these digital devices are essentially interconnected, bringing about an exponential growth in connectivity. Revolutionary computing advances like breakthroughs in the miniaturization of integrated circuits, in data processing and transmission speeds and storage capacities, the advent of intelligent systems and robotics, the growing comfort of ergonomic human–computer interaction, mean that devices not only pervade our environment in an unprecedented way, linking people, objects and information in a novel manner, they also bring with them the next generation of digital disruption possibilities and, indeed, a sea

Ambassador Henning Wegener, a retired German diplomat, is Chairman of the World Federation of Scientists' Permanent Monitoring Panel on Information Security.

change in how we must view and deal with information security. The rapid progress of a huge range of wireless techniques, including all-pervasive sensors and radio-frequency identification technologies, adds to the dimension of new vulnerabilities.

The benefits of new technologies can be undercut by digital disruption, by the negative use of such technologies. These uses are wide-ranging, and include cyber-attacks, viruses, spam mail with embedded Trojan horses and other malware, sabotage of data systems, etc., but also the transmission of hidden information (e.g. for information exchange among criminal organizations). Modern, integrated societies are thus made fragile by their dependence on new technologies. The threats from cyberspace are of major relevance for the functioning and security of the world system: we vitally depend on the absence, or at least adequate harnessing, of cybercrime, cyberterrorism and cyberwar.

We vitally depend on the absence, or at least adequate harnessing, of cybercrime, cyberterrorism and cyberwar.

A quantum leap in the level of threat

The leap in the level of threat is not new, it is in fact self-evident. Cybercrime and cyber-insecurity have been a topic of analysis, debate and public and private action since at least the early 1990s, reflecting in each phase the growth curve of cyber-risks. The new and troubling fact is, however, that the cybercommunity is at this juncture entering an era in which there appears to be a quantum leap in exposure to major risk. The age-old race between attack and defence, where attackers tend to be ahead in sophistication and vigour, is further skewed in the cyberworld as the attacker is totally independent of time and place, and is in possession of rapidly renewable arsenals of means of attack that potentially produce global harm. The currently observable sophistication and intensity of attack techniques as well as the organizational level of perpetrators is truly breathtaking. It can now seriously be questioned whether the ongoing battle for cybersecurity can still be won.[2]

As vulnerabilities increase, the threat appears to rise even more steeply. The rate at which new species of virus—often 20 per day—are emerging and then spreading, the overwhelming presence of spam (lately reported to reach more than 90% of total e-mail traffic), the sophistication of phishing sites and the spread of implanted botnets (from which paralysing Distributed Denial of Service attacks can be waged) are phenomenal. Every day, tens of thousands of computers are recruited into secret networks and, hidden from their owners, are able to spread spam or viruses or commit massive data theft. In some countries, more than 70% of all personal computers are reported to be thus infected.

The main perpetrators of these crimes are no longer playful hackers, but well organized conglomerates with criminal intent and vast economic and technological prowess. They are increasingly able to achieve dominance in the swift development of new attack software, which soon finds its way to the black market. Beyond profit, these groups may be driven by more sinister political motives. It is not difficult to imagine how this damage potential can be diffused to cyberterrorists or states intent on cyberwar.

The threat to international peace and security

There are three main categories of harm that can flow from cyber-attacks: their economic consequences, disruption to critical infrastructures, and threats to national security and the capabilities of military and defence systems and first responders.

Economic damage caused by cybercriminals already reaches mind-boggling proportions. Among other reasons, industrial secrecy, and even lack of awareness of the crimes, make exact global figures difficult to come by, but estimates calculate annual economic losses as reaching tens of billions of dollars. Cyber-attacks against critical infrastructures that increasingly depend on ICTs (dams, aviation and air control, electricity grids, pipelines, factories with dangerous or sensitive production processes, the banking system, national health systems, essential government and industry databanks, etc.) also pose a serious problem. These infrastructures are typically in private hands and especially vulnerable because most of their distributed control systems (DCS) and supervisory control and data acquisition systems (SCADA) are connected to the Internet, from where they can be disrupted. Moreover, the growing interdependence of these systems means that cyber-attacks can produce immediate, grave repercussions throughout national economic and political systems, and even significant cross-border effects. Cumulative attacks on various structures may, through instant chain reactions, cause the damage to grow manifold.

State and non-state actors are now in a position to directly or indirectly commit cyber-attacks against the national defence assets of another state, disabling its electrical and communication systems, blocking emergency call systems, interfering with the acquisition of intelligence, the functioning of weapon systems or command and control procedures. Even more disconcerting is the potential, or rather the likelihood, of a combination of attacks that would *simultaneously* impair economic interests, critical infrastructure and military and defence capabilities.

Cyberwar, the use of "information weapons", is a very real technique. The digital breakdown in Estonia in April 2007 as a consequence of massive, manifestly well orchestrated, external attacks on private and public networks, may well be the first incident of real cyberwar characteristics. As this event demonstrates, combined attacks are now a distinct possibility. If one projects these vulnerabilities onto the current threat of international terrorism, ominous scenarios become menacingly plausible. Information security and the concepts of national and international peace and stability are today intrinsically linked.

The case for international cooperation

The cyberthreat is asymmetric; it is inherently invisible, non-linear, and it has the potential to disrupt the social fabric and essential assets of one or more states, all with a minimum of input and investment. The problem is global and will not be resolved by the efforts of just one state or group of states, or even by regions. The Internet knows no frontiers, and attacks may come from distant and undisclosed locations, or out of countries where the regulatory framework is insufficient. Tracking and tracing attackers across a borderless cyberworld, and holding them accountable, requires multilateral action that transcends jurisdictions and national boundaries. A united effort by the international community and harmonized or compatible measures by all states are required. Tracking and tracing requires cooperation encompassing the legal, political, technical and economic realms. Safeguarding information security is a universal challenge.

National governments and the international community have been working on telecommunication and IT security standards, frameworks for critical infrastructure protection and anti-spam strategies. In addition, a potent cybersecurity industry has emerged. Cybersecurity is good business and the industry's growth rate is staggering. Sophisticated spam filters, more secure antivirus software, anti-spyware, encryption techniques, secure quantum networks and protected high-speed data transport lines constitute only a partial list of IT security industry achievements. Yet many of these measures are powerless against new varieties of malware that the highly creative attack systems regularly introduce. Despite these efforts, the current attack–defence balance is far from reassuring, and it is collective, international action that is now urgently required.

The challenge to the international community is complex and comprehensive both in the range of subjects to be addressed and the number of actors involved. The management of cyberspace comprises a comprehensive regulatory framework, including Internet governance, and involves intergovernmental mechanisms, governments, the private sector and civil society—jointly and conveniently referred to as the "stakeholders" of the cyberworld.

A nascent international regime

Self-interest, the apparent and growing need to stem cyber-insecurity and promote risk mitigation, has propelled all sectors of society in most countries to confront the cyber-challenge: so many efforts are being undertaken that it would be futile to provide even a schematic list of pertinent activities and actors around the globe.

A challenge of such complexity does not allow for easy streamlining or simple organizational structures. There can be no unified organizational solutions able to respond to the question "who is in charge?", but there are possibilities for creating an organic relationship between the existing and necessary multitude of actors based on unity of purpose. A homogeneous command structure cannot be put in place, but the development of a model of shared responsibility and operational work modes is possible. The objectives must be to heighten worldwide awareness of cyber-risks, to maximize synergies, to provide for processes of mutual learning and information sharing, and to establish mechanisms of coordination. Equally important are regulatory requirements: the need to harmonize and enforce globally valid codes to fight cyber-attacks, leaving no loopholes, and the necessity to provide overall orientation for the further evolution of the cyberworld. There is a pressing need to fill gaps in cyberprotection, particularly in developing countries; nascent information structures are especially vulnerable, and thus capacity-building in developing economies must go hand in hand with security-building.

The theoretical construct that best meets these needs may be that of an international regime, as developed in regime theory during the 1980s.[3] The essence is that an international regime is appropriate when the behaviour of international actors needs to be coordinated around a defined issue, however complex. Regimes, clustered around a central institution—or institutions—serve crucial functional needs in a "given area of international relations" and are based on explicit or implicit "principles, norms, rules, and decision-making procedures around which actor expectations converge";[4] this also includes procedures for conflict solution. Inclusiveness is an important ingredient of regimes. The international financing system, the non-proliferation regime, the Kyoto Protocol and other environmental arrangements, the debt financing and rescheduling mechanisms for developing countries and many other clusters of arrangements have at various times been defined as international regimes. Some years past, Goodman et al analysed the civil air transport regime, centred on the International Civil Aviation Organization and feeding on a series of international aviation security treaties, suggesting that this regime could be a model for international cooperation on cyberterrorism and cybercrime.[5]

In 2001, the World Federation of Scientists first made the case for a "universal order of cyberspace" as an overriding management concept for mastering the digital era and for successfully harnessing the threat landscape, from cybercrime to cyberwar.[6] This proposition is fully compatible with the regime concept; the more so since the authors have also developed the idea of a globally negotiated and comprehensive Law of Cyberspace as the backbone of their proposed universal order. This concept has since been further elaborated in a publication from the United Nations Institute for Training and Research, which makes the argument that cyberspace is part of the common heritage of mankind, and that unimpaired access to its benefits is a legitimate right of all.[7] The regime concept appears to be a fertile device for ordering national and international cyberspace activity, and deserves further exploration.

Leadership of the cyberspace regime

Among the package issued by the World Federation of Scientists is the recommendation that, because of its universal character, the United Nations system should have the leading role in intergovernmental activities concerning the functioning and protection of cyberspace. There appears to be no opposition to this concept, indeed cybersecurity has rightly become a matter of substantial concern to the UN General Assembly, where a series of resolutions and activities, the most recent being resolution 61/54 "Developments in the field of information and telecommunications in the context of international security", have underlined that existing and potential threats in the field of information security require multilateral attention and the re-examination of relevant international concepts.

Fortunately, the United Nations appears ready to take on a leading role, as demonstrated by the two sessions of the World Summit on the Information Society, or WSIS, held in Geneva in 2003 and in Tunis in 2005. The WSIS has been one of the most necessary and successful summit meetings ever held under the auspices of the United Nations. In the final (consensus-based) documents of the two conference phases it has provided an incipient codification of the principles that are to govern the cyberworld—a promising building-block for a universal order of cyberspace. The Tunis Agenda on the Information Society particularly places due emphasis on the issue of cybersecurity. Moreover, in its clear assignment of tasks to the various members of the UN family, the WSIS has helped to clear up the somewhat murky competencies within the UN system. In the Annex to the Tunis Agenda, various "action lines" entrust concrete tasks to various agencies according to their area of competence. It is particularly noteworthy that there is a precise follow-up mechanism. Not only are the recipients of the action line assignments under a clear mandate, but General Assembly resolution 60/252 of 27 March 2006 asked the Economic and Social Council (ECOSOC) to oversee system-wide follow-up to the summit outcomes through annual deliberations until 2015 (when the next WSIS is due). The Commission on Science and Technology for Development (CSTD) is to be the focal point for the summit follow-up, reporting to ECOSOC. ECOSOC has fleshed out CSTD's mandate (resolution 2006/46, 28 July 2006): the commission is to be strengthened, and is to practise a multi-stakeholder approach as well as include other international organizations in its work. Both this policy of inclusiveness and the clarity of the mandate are welcome. The CSTD is to be serviced by the United Nations Conference on Trade and Development Secretariat, which, as its annual reports on the information economy demonstrate, possesses a considerable grasp of cyberspace issues. Work has already begun: the CSTD has agreed a programme of work to review progress made in WSIS outcomes.[8] The United Nations Group on the Information Society has been established by the General Assembly for internal coordination of WSIS implementation work within the UN system. Its members are all members of the UN System Chief Executives Board.

The foundations for a coherent cyberspace regime appear to be in place.

Important management and competency questions have thus been taken in hand, and the foundations for a coherent cyberspace regime appear to be in place.

WSIS Action Line C5, "Building Confidence and Security in the Use of ICTs", has been given to the International Telecommunication Union (ITU) as the sole facilitator agency. ITU therefore deserves special emphasis not only as the organizer of the WSIS, but as the main multilateral repository of the cybersecurity issue. ITU, because of its unique technical expertise and staff resources, along with its inclusive combination of public and private interests (700 ITC-related companies and organizations take part in ITU's work as members or associates) is especially apt for exercising a coordination role and providing leadership. The multi-stakeholder approach required for tackling cybersecurity is within ITU's traditions. With the recent adoption of its Global Cybersecurity Agenda—which aims to curb cybercrime within two years—and the establishment of its online Cybersecurity Gateway, ITU is impressively filling its assumed leadership role in cybersecurity issues and WSIS implementation. It has the potential to become the central global information forum for these activities—the (so far annual) all-stakeholders meetings on Action Line C5 may well become the global focus for raising awareness, sharing state-of-the-art information and prompting collective action.

Among other things, the Global Cybersecurity Agenda advocates the development of interoperable legislative frameworks. ITU could become a powerful instrument for furthering globally harmonized legal standards for cybercrime and law enforcement—it is hoped that the union will work in close cooperation with the Council of Europe (whose Convention on Cybercrime is the benchmark document for an emerging universal system of cybercrime law and law enforcement), the European Union (EU), the Organisation for Economic Co-operation and Development and the United Nations Office on Drugs and Crime, all of which have been active in this area.

A further important component of the Global Cybersecurity Agenda is the emphasis on building ICT security in those developing countries that are most vulnerable and thus the weakest link in the cyberworld. Ultimately, its growing expertise will enable the ITU to turn into the "International Information Technology Agency", the necessity of which has been underlined and frequently recommended.

Work still to be done

The determined stance and clear policy orientations of the ITU leadership are a particularly positive element in the emerging international cybersecurity regime. However, to make the regime truly effective, further requirements must be met. In the first place, a seamless security net will naturally depend on the cooperation of *all* national governments and the speed with which they do their share in formulating a corresponding cybersecurity policy and in practising "governance for security", raising civil awareness, enacting legislation and tuning up their law enforcement machinery. It will further depend on whether all other stakeholders, including the private sector, will accept the offer of inclusiveness and participate fully.

There are important networks that do not yet figure in the activities of ITU or other multilateral actors. International law enforcement organizations like Interpol and, in the European context, Europol, should assume a greater role in cybercrime matters. They should build a relationship with ITU as the multilateral lead agency and have stronger functions and investigative powers. ITU plans to promote the establishment of national cybercrime response teams; it should therefore concern itself with promoting universal introduction of the "24/7 network" pioneered by the Group of Eight and since adopted by 57 states. Now also part of the Council of Europe's Convention on Cybercrime, this network consists of points of contact available round-the-clock for alert information and mutual assistance in ICT-related cases. Computer Emergency Response Teams (CERT) comprise another important alert and response network that is now active in most countries. First created by Carnegie Mellon University in the United States, CERTs can be found within public or private organizations, and are coordinated at the international level by the Forum of Incident Response Security Teams. CERTs are certainly within the purview of ITU, and their activities must be included in any cybersecurity regime. ITU should work to introduce CERTs in countries where they are not yet operating—several international bodies (the EU and Asia-Pacific Economic Cooperation) already provide technical assistance to this effect. The Internet Governance Forum (IGF) was created by the WSIS and includes Internet security in its mandate. The IGF reports to the UN Secretary-General: it is a multi-stakeholder forum for policy dialogue, allowing for openness and flexibility. It has no negotiating mandate, but its work can lay the foundations for activity to be taken on by other institutions. The IGF's work relates closely to that of the ITU and the two bodies should be working together; indeed, the Secretary-General of the ITU will be present at the next IGF meeting, to be held in November 2007. The Global Alliance for ICT and Development,[9] established to promote effective use of ICT in development activities, is also shaping up as an open, multi-shareholder discussion forum, but has—for less than plausible reasons—excluded information security from its agenda, and accordingly is of lesser importance in the architecture of a cybersecurity regime.[10]

There remains one outstanding issue to be considered prominently if a comprehensive international regime is to be created: the development of international law to encapsulate cyberwar or lesser transborder hostile actions by states or non-state actors. It is presently unclear how traditional international law pertains to cyber-attacks and how "information weapons" are to be dealt with in the laws of armed conflict; the World Federation of Scientists has repeatedly attempted to pierce this veil of obscurity, but responses in the literature and multilateral action have so far been scarce. The cybersecurity issue requires examination and interpretation of the United Nations Charter (which was of course not drafted with the cyber-age in mind). How do cyber-attacks and information warfare relate to the terms of the charter? How do we define the new terminology that comes with new technology? A key concept needing elucidation is the Charter term "armed attack". Could the use of ICT to cause, or entail, death and destruction in another state be considered such? A comprehensive international Law of Cyberspace needs to address cyber-warfare, and recent events highlight the urgency of the matter. It is thus fitting, and indeed necessary, that UN organs turn their attention to the issue and help map the international laws of war in cyberspace.[11]

The WSIS has not yet dealt with this important topic and not assigned competencies. International work on this issue is urgent and will require the involvement of many bodies, as it concerns definition of terms and interpretation of legal documents. The UN General Assembly, including its First and Sixth Committees, and the International Law Commission should acknowledge and accept the challenge of developing an appropriate legal framework defining legitimate and illegal cyber-actions by states and non-state actors. The international scientific community should, as a matter of priority, examine scenarios and criteria and international legal sanctions.

This is an important gap to be filled. In general terms, however, the good news is that an international cyberspace regime has been designed and is already functioning. There is much more work to be done.

Notes

1. Ulrich Beck, 1999, *World Risk Society,* London, Polity Press.
2. Part of this argument has been collected from the assessment of the state of cyberthreats during the 2nd ITU Facilitation Meeting for WSIS Action Line C5 held in Geneva, 14–15 May 2007. (Meeting Report, document ALC5/2007/Meeting Report v.2, 17 May 2007, at <www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/meetingreport.pdf>).
3. See Robert O. Keohane, 1982, "The Demand for International Regimes", *International Organization,* vol. 36, no. 2, pp. 325–355; Stephen Krasner (ed.), 1983, *International Regimes,* Ithaca, NY, Cornell University Press.
4. Stephen D. Krasner, 1983, "Structural Causes and Regime Consequences: Regimes as Intervening Variables", in Krasner, op. cit., p. 1.
5. Seymour E. Goodman, H.H. Whiteman, Mariano-Florentino Cuéllar, 1999, "The Civil Aviation Analogy", in Abraham D. Sofaer and Seymour E. Goodman (eds), *The Transnational Dimension of Cyber Crime and Terrorism,* Stanford, CA, Hoover Institution Press, at <www.ituwiki.com/index.php?title=The_Transnational_Dimension_of_Cyber_Crime_and_Terrorism>.
6. World Federation of Scientists, 2003, *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar,* document WSIS-03/GENEVA/CONTR/6.
7. Ahmad Kamal, 2005, *The Law of Cyber-Space: An Invitation to the Table of Negotiations,* Geneva, UNITAR, at <www.unitar.org/documents/thelawofcyberspace.pdf>.
8. CSTD, *Report on the Tenth Session,* 21–25 May 2007, UN document E/2007/31.
9. The Global Alliance for ICT and Development is successor to the UN ICT Task Force.
10. A Group of Governmental Experts tasked to study the threats to information security was put in place by the UN General Assembly in 2003. However the group, which met in 2004 and 2005, failed to reach consensus upon a final report, mainly because of the breadth of its mandate. With a narrower mandate, and a clearer agenda, it is hoped that the next group will be in a position to make a more significant contribution to cybersecurity matters. See General

Assembly resolution 58/32 of 8 December 2003, UN document A/RES/58/32, 18 December 2003, for the group's mandate, and *Report of the Secretary-General,* 5 August 2005, UN document A/60/202, for the conclusion of the group's work.

11. For more on international law and information security, see the article by Sergei Komov, Sergei Korotkov and Igor Dylevski in this issue of *Disarmament Forum*. In addition, Gregory D. Grove, Seymour E. Goodman and Stephen J. Lukasik, 2000, "Cyber-attacks and International Law", *Survival,* vol. 42, no. 3, January, remains a seminal article on the legal implications of cyberwar. See also the recommendations and discussion of cyberwar in World Federation of Scientists, 2003, op. cit.; Vitali Tsygichko, no date, *Cyber Weapons as a New Means of Combat,* and Andrey Krutskikh, no date, *International Information Security and Negotiations,* both at <www.itis-ev.de/infosecur>; and International Centre for Scientific Culture World Laboratory and World Federation of Scientists, 2005, *Information Security in the Context of the Digital Divide,* document WSIS-05/TUNIS/CONTR/01-E, pp. 30–35.

UNIDIR FOCUS

ACTIVITY

Disarmament Insight: thinking differently about human security

Multilateral disarmament practitioners are busy people. Because of myriad demands on their time and attention it can sometimes be difficult to convey to them the implications of new policy research that could make their work more productive.

In late 2006, UNIDIR's project on Disarmament as Humanitarian Action: Making Multilateral Negotiations Work (DHA) began collaborating on the Disarmament Insight initiative with the Geneva Forum. The Geneva Forum is a joint initiative of the Quaker United Nations Office (QUNO) in Geneva, UNIDIR and the Programme for Strategic and International Security Studies (PSIS) of the Graduate Institute of International Studies.

The DHA project's work has revolved around two related themes: showing how humanitarian perspectives can assist disarmament and arms control work, as well as looking more broadly at new tools and perspectives to help multilateral negotiators reframe and respond effectively to disarmament challenges.

Under the rubric of "thinking differently about human security", the Disarmament Insight initiative aims at engaging with multilateral practitioners and others on the findings of the DHA project's research and related themes, for instance drawing from its three volumes of research published by UNIDIR in 2005 and 2006.

As well as symposia with multilateral practitioers and other activities, a number of Disarmament Insight web resources have been developed. These are accessible online at <www.disarmamentinsight.blogspot.com>.

Disarmament Insight web resources include links to the content of DHA's published volumes and information about the project, a topical research blog updated every few days (on which visitors can post their comments) and podcasts of speakers from Disarmament Insight events. Recent podcasts include:

- Professor Frans de Waal, one of the world's foremost primatologists, explaining to disarmament diplomats what they can learn from "War and Peace and Primates"; and

In each issue of *Disarmament Forum*, UNIDIR Focus highlights one activity of the Institute, outlining the project's methodology, recent research developments or its outcomes. UNIDIR Focus also describes a new UNIDIR publication. You can find summaries and contact information for all of the Institute's present and past activities, as well as sample chapters of publications and ordering information, online at <www.unidir.org>.

- Professor Paul Seabright, economist and author of The Company of Strangers: A Natural History of Economic Life, exploring with multilateral practitioners what we know about levels of armed violence, and what we might learn from behavioural economics and neuroscience that would help them in their work.

For more information, visit <www.disarmamentinsight.blogspot.com>.

NEW PUBLICATION

International Assistance for Implementing the United Nations Programme of Action on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects: Case Study of East Africa

Small arms and light weapons (SALW) are a serious threat to the security and development of East Africa. However, Burundi, Kenya, Rwanda, Tanzania and Uganda are tackling the illicit trade in SALW, developing new legislation, defining national objectives, and in some cases implementing action plans and coordinating with the Regional Center on Small Arms and Light Weapons and the East African Community. Yet due to the lack of capacity and the extent of the SALW problem in the subregion, international assistance in implementing SALW programmes is necessary. Most SALW assistance received between 2001 and 2005 went toward disarmament, demobilization and reintegration (DDR) programmes; only 5% of assistance was used to implement other SALW projects, primarily in Kenya, Tanzania and Uganda. Each of the five states presented in this case study are at different levels of implementation and have different capacities available to implement the UN Programme of Action on the Illicit Trade in Small Arms and Light Weapons.

By early 2008, the states will have passed revised policies and legislation on SALW, and thus assistance in awareness-raising on, training in and enforcement of the policies and legislation will be key. Strengthening the capacity of the National Focal Points is a particular priority for Burundi and Rwanda, and improving the capacity and resources available along borders and at border entry points, record-keeping, stockpile security and management, and marking of arms are among the top needs consistently identified by states in the subregion. In addition to presenting the results of the case study on international assistance in East Africa, this report includes some general policy recommendations for improving resource mobilization. Individual profiles of each state, outlining SALW action and needs for assistance, are presented at the end of the report.

This case study was conducted as part of UNIDIR's work on "International Assistance for Implementing the Programme of Action on the Illicit Trade in Small Arms and Light Weapons", which aims to develop a mechanism that will help states identify the types of assistance they require to implement the PoA, and make that information available to potential assistance providers.

International Assistance for Implementing the United Nations Programme of Action on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects: Case Study of East Africa

Kerry Maze and Hyunjoo Rhee

Electronic publication available at <www.unidir.org>

40 pages

UNIDIR

Free of charge