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.