**Ensuring Cyberpeace in a New World Order**

1. **Introduction**

Information and Communication Technologies (ICTs) have become an integral part of everyday life for many people of the world. Digital communications, networks and systems provide vital resources and indispensable infrastructure throughout the global community, necessities without which many populations could not flourish or even survive. These structures and systems represent a new domain, and with it come new challenges for preserving peace and stability. Without mechanisms for ensuring peace, cities and communities of the world will be susceptible to attacks of an unprecedented and limitless variety. Such an attack could come without warning. Suddenly, computers and cell phones will cease to function, ATM (Automatic Teller Machine) screens will stare blankly at customers, air traffic control, railroad and motor traffic systems will leave highways, bridges and waterways in chaos and perishable goods stranded far from hungry populations. With the loss of electricity, hospitals, houses, shopping centers, whole communities will tumble into darkness. Government authorities will be unable to take stock of the damage, communicate with the rest of the world to spread word of the crisis or protect their vulnerable citizenry from subsequent attacks. This is the intractable plight of a community paralyzed by the instantaneous loss of digital networks. This is the potential devastation of a new kind of war, a “Cyberwar.”

1. **A New Domain: Cyberspace, Security and Warfare**

The threat of cyberwar now looms larger than ever. Today, technological advancements and growing digital infrastructure bind whole populations to complex, intertwined systems. Demand for Internet and digital connectivity calls for ever-increasing integration of ICTs into products that previously functioned without it, such as cars, buildings and even control systems for vast power and transportation grids. Electricity supply, transportation systems, military services and logistics – virtually all modern services depend on the use of ICTs and the stability of cyberspace. “Cyberspace” is the physical and conceptual realm in which all these systems exist. Therefore, “Cyberwar” may be broadly understood as a war fought in cyberspace using and targeting ICTs.[[1]](#footnote-1) Rapidly increasing dependence on smart grids and other Internet-based control and monitoring systems places the heart of energy, transportation and defense resources within reach of those who seek to wreak havoc on government and civilian populations.[[2]](#footnote-2) Thus, as global reliance on ICTs grows, so does vulnerability to attacks on critical infrastructures through cyberspace. With all of these changes, enhancing cybersecurity and protecting critical information infrastructures are now essential elements of each nation's security and economic well-being.

Although the exact contours of a “cyberwar” are still undefined, substantial attacks against information infrastructure and Internet services in the last decade provide some sense of the potential shape and scope of a conflict in cyberspace. Attacks in Georgia,[[3]](#footnote-3) Estonia,[[4]](#footnote-4) South Korea and the United States[[5]](#footnote-5) have been linked with cyberwarfare. Multiple blackouts in Brazil have been connected to cyber attacks and in 2008 hackers broke into the government’s web site and took control of it for over a week.[[6]](#footnote-6) The blackouts in Brazil illustrate the possible breadth of emerging kinds of cyber attacks: reports liken the scene to a science-fiction film, with subway trains, traffic lights and the world’s second-largest hydroelectric power producer, the *Itaipu* dam, brought to a crashing halt and more than 60 million people affected.[[7]](#footnote-7) Cyberwar might also involve the private sector. Web service giants like *Google*[[8]](#footnote-8) and *Twitter*[[9]](#footnote-9) already experienced attacks in 2009 and, as early as 2000, denial-of-service attacks were launched against well-known companies such as *CNN, Ebay* and *Amazon*.[[10]](#footnote-10) As a result, some of the services were not available for several hours or even days. Hackers have targeted airport control systems, disabling critical equipment like phone services and runway lights.[[11]](#footnote-11) By some counts, more than six countries have experienced cyber assaults in the past three years and at least 34 private companies were attacked in the early months of 2010 alone.[[12]](#footnote-12) Though these security concerns are serious, it is not too late to stave off potentially catastrophic scenarios by creating safer products, practices and standards through a collaborative international effort.[[13]](#footnote-13) Making the Internet safer and protecting ICTs from disruption and destruction must be priorities if we are to protect civilian populations, ensure the effective functioning of basic structures and provide for the continued development of new services.

1. **Cyberwar**
2. **Definition and Concept**

The concept of cyberwar encompasses the targeting of not only military capabilities and systems, but also a society’s vital infrastructure—including Smart Grids and supervisory control and data acquisition (SCADA) networks—that allows it to function and defend itself. While using a different medium (cyberspace and the ICTs operating in it), opponents can still deploy weapons and engage in an offensive-defensive conflict much like traditional warfare. Cyberwarfare tactics typically involve data collection or infiltration of computerized systems to cause damage to critical systems.[[14]](#footnote-14) Potential cyber weapons include: electromagnetic pulse weapons, compromised counterfeit computer software, wireless data communications jammers, computer viruses and worms, cyber data collection exploits, computer and networks reconnaissance tools and embedded Trojan time bombs.[[15]](#footnote-15) Increasing reliance on smart grids leaves many countries’ power supplies particularly vulnerable to attack. Smart grids are digitized systems which connect utility supplies to a central monitoring network, often called a supervisory control and data acquisition, or SCADA, network. SCADA networks gather information about power use and supply, while smart grids provide a digitized channel for that information to flow between consumers and suppliers.[[16]](#footnote-16) These technologies are now used for a wide variety of processes and systems, including: water management systems, gas pipelines, electrical power transmission and distribution, wind power systems, mass communication systems, manufacturing, production, mass transit systems, environmental control systems, air traffic control and traffic lights.[[17]](#footnote-17) More and more, suppliers are connecting smart grids to the Internet in order to allow for remote access and increased functionality.

While connected grids offer substantial benefits, such as reduction of energy waste and faster communication between customers and providers, they also centralize data and control of huge power grids on a network that has multiple access points. With more endpoints and more interconnected networks, smart grids and SCADA networks provide numerous ways for attackers to infiltrate them.[[18]](#footnote-18) For example, a smart meter (an electrical meter connected to the grid) can be hacked and infected fairly easily, and it can then be used to spread a worm to other meters and eventually cause the power grid to surge or shut off.[[19]](#footnote-19) Though many firms seek to secure their grids by isolating control centers from other networks (a technique called “air-gapping”), these attempts to completely seal off certain components often fail, often unbeknownst to the administrator of the system.[[20]](#footnote-20) Logic bombs are another way attackers might disrupt or even destroy a smart grid; hackers might infiltrate the grid to hide malicious software in it, waiting to activate these bombs at a later time for a coordinated assault or to cause limited power failures.[[21]](#footnote-21) Such bombs create an additional security problem because they could be detonated accidentally or by a different hacker who discovers them at a later date.[[22]](#footnote-22)

Already, countries that have invested in smart grids are reporting attempted attacks and probes numbering in the thousands per day.[[23]](#footnote-23) By some estimations, cyber attacks are the greatest threat to national power-generation grids.[[24]](#footnote-24) A remote attack could very well target physical infrastructure like power generators and transformers, causing them, in essence, to self-destruct.[[25]](#footnote-25) Such an attack would most likely have long-range consequences, as power companies do not usually store expensive replacement parts, which can take months to manufacture and deliver.[[26]](#footnote-26) An attack on a smart grid would not only leave customers without power, but it would also create massive financial damage. Power generators can run in the multi-million dollar range and overall investment into smart grids runs in the tens of billions for some countries.[[27]](#footnote-27) In addition to the potential for extensive physical destruction and immediate financial loss, the threat of future cyber attacks undermines confidence in existing and new technologies like smart grids and, in turn, in the reliability of electronic, financial and health resources. This loss of confidence alone could cause tremendous societal and economic upheaval.[[28]](#footnote-28) The development of smart grid use with nuclear reactors (and nuclear weapons facilities) creates even greater risks and potential damage. Beyond traditional attack and defend strategies, cyberwarfare might also entail attacking an entity or country’s internal systems in order to temporarily distract or hamper them, as opposed to directly damaging them.[[29]](#footnote-29) A country might choose this kind of cyber attack if, for example, it wants to disable allied support of a targeted opponent long enough to achieve a specific objective.[[30]](#footnote-30)

1. **Unique Features and Impact of Cyberwar**

Although cyberwar could resemble traditional warfare in some ways, the unique characteristics of cyberspace bring new and unforeseen dimensions as well. Because systems in cyberspace are linked by computers and communication networks, the disruption caused by a ICT-based attack goes beyond the failure of a single system and often beyond national boundaries. Many data transfer processes affect more than one country and many Internet services are based on services from abroad; for example, host providers may offer webspace for rent in one country based on hardware in another. Even short interruptions to services could cause huge financial damages to e-commerce businesses. Not only civil communications could be interrupted by attacks, the dependence on ICTs is also a major risk for military communications. Unlike more traditional combatants, cyber offenders do not need to be present at the place where the effect of the attack occurs or even where it appears to originate. And while carrying out the attack, the offenders can use the means of anonymous communication and encryption technology to hide their identity.[[31]](#footnote-31)

Moreover, software tools, which are widely available over the Internet, are being used to automate attacks. With the help of such software and preinstalled attacks, a single offender can attack thousands of computer systems in a single day using one computer. If the offender has access to more computers – e.g., through a botnet – s/he can increase the scale still further. For example, analysis of the attacks against government websites in Estonia suggests that they were committed by thousands of computers within a “botnet” or group of compromised computers running programs under external control.[[32]](#footnote-32) Botnets also make it more difficult to trace the original offender, as the initial traces only lead to the members of the botnets. Current analysis suggests that up to a quarter of all computers connected to the Internet could be infected with software making them part of a botnet. Software tools also simplify attacks, allowing less experienced computer users or less advanced military outfits to commit cyber attacks. In addition, ICT-based attacks are generally cheaper than traditional military operations and can be carried out by even small states. Now, even a state with historically weaker military capabilities has the capacity to severely cripple critical infrastructure through cyber attacks. This potential for asymmetry makes cyberwar appealing as a strategic way to level the playing field in “otherwise David versus Goliath scenario[s].”[[33]](#footnote-33) The fear of cyberwar, reinforced by the actual (albeit limited) occurrence of cyber attacks, undermines public confidence in ICTs. Thus, the potential psychological ripple effect of cyber conflict could have widespread implications for disrupting the effective use of new technologies and hampering progress in many sectors.

1. **International Responses to Cyberwar**
   * 1. **National Policies and Approaches**

Countries around the world are responding to the new threat of cyberwar in a variety of ways. Although some states are just beginning to address the issue of cybersecurity,[[34]](#footnote-34) most governments at the very least recognize the need for reallocation of resources and reform of national security strategies on some level. Many nations are increasing funding, research and tactical and diplomatic resources to improve their cybersecurity.[[35]](#footnote-35) Some countries engage in “air-gapping”—attempting to isolate particular networks by not linking them to other systems—to protect critical information structures and systems from attack.[[36]](#footnote-36) The following section assesses the different approaches adopted by various states.

* 1. **Incorporating cyber capabilities into conventional warfare strategy**

Some countries are exploring a conventional warfare approach when it comes to cyber tactics, building up cyber offensive weapons and defensive capabilities as well. They view cyber weapons as “force multipliers,” to be used primarily in conjunction with more traditional military actions in order to significantly increase their combat potential.[[37]](#footnote-37) Over recent years, the Internet has become an important medium for information and propaganda exchange during armed conflicts. In this regard, many countries view information sabotage on the Internet as a form of military aggression against public morale and they are thus prepared to meet cyber attacks with military force. [[38]](#footnote-38) Recent incidents involving the leaking of classified military documents illustrate why states worry about the potential consequences for morale and public support.[[39]](#footnote-39) Some state officials have indicated in the past that they would consider information warfare tactics to be military actions, whether or not they resulted in casualties, and a military response could therefore be warranted.[[40]](#footnote-40)

* 1. **Cultivating cyber tactics as a national resource**

Through their reallocation of resources, funding and strategic planning, many countries are treating their digital infrastructure and ICTs as a national resource or strategic asset. Some countries have even explicitly articulated this as a new national policy.[[41]](#footnote-41) Countries have shifted budgetary resources towards cyberspace initiatives, setting aside considerable sums for research and development of cyberwarfare capabilities.[[42]](#footnote-42) Several governments have articulated and begun pursuing integrated national plans to address the new cyber threat, mobilizing multiple sectors and completely transforming resources and strategy.[[43]](#footnote-43) This kind of transformation could include training (or re-training) military personnel, revamping intelligence services to focus on collecting relevant scientific and technological information and conducting cyberwarfare simulations and military exercises, all with specific attention to the applications of information technology.[[44]](#footnote-44) Several countries have initiated national competitions to identify and recruit the strongest cyber-minds among their civilian population.[[45]](#footnote-45) Domestic industries are also pushed to develop improved technological capabilities in support of the new military strategy. Some governments are also working to cultivate a pool of private civilian hackers who could be called upon if necessary.[[46]](#footnote-46) These “hactivists” may be tech-savvy individuals or even former illegal hackers recruited and trained to use their skills for national security purposes.[[47]](#footnote-47) Some countries may even use proxies, hired hackers and specialists from other countries who act on their behalf.[[48]](#footnote-48) All of these changes demonstrate a departure from more reactive strategies to cyber threats and a reorientation around the development of proactive information warfare tactics to effectively act under hi-tech conditions.[[49]](#footnote-49)

* 1. **Building cyber military outfits**

Several countries have responded to the new threat of cyberwar by allocating large numbers of military personnel to the task of virtual combat.[[50]](#footnote-50) This policy shift could involve the development of Internet warfare teams dedicated to cyber-security, which could be integrated into other intelligence agencies,[[51]](#footnote-51) or even the creation of entirely new sectors within the military structure dedicated to cyber activity.[[52]](#footnote-52) These new military outfits set out to integrate and prepare military resources for full-spectrum cyberspace operations.[[53]](#footnote-53) While their primary focus is often the protection of military networks and conducting military operations in cyberspace, they may also be charged with securing private networks, which power large portions of many military operations, as well.[[54]](#footnote-54)

* 1. **Using cyber tactics to level the playing field**

By perfecting information and electronic warfare tactics, some countries hope to level the playing field with nations that rely on software and computer systems to mobilize their conventional armed forces. This transition involves investment in new automated command systems, including hardware such as fibre optic cables, satellites and high-frequency digital radio systems, as well as an increased focus on space, air, naval and ground-based surveillance systems.[[55]](#footnote-55) Some governments already utilize ICTs, in conjunction with tech-savvy military personnel, to monitor national borders.[[56]](#footnote-56) New cyber-oriented strategies might rely even more heavily on these resources, and their attendant automated systems, to secure borders. Other tactics might include command and control operations that focus on disrupting enemy information flow and the targeting of enemy ICT infrastructures to damage and destroy critical machinery, networks and data.[[57]](#footnote-57) These changes focus on attacking potential adversaries’ weak points – namely, their reliance on cyberspace and new technologies. Countries that have the strongest traditional and cyberwar capabilities may actually be most vulnerable because of the technology that fortifies them, which is susceptible to new kinds of attack like logic bombs and hacking.[[58]](#footnote-58) By capitalizing on the potential asymmetry of actions in cyberspace, countries hope to neutralize the military capabilities of their adversaries.[[59]](#footnote-59)

* 1. **Educating citizens and raising awareness of cybersecurity problems**

Many governments recognize public education and awareness as powerful methods of cyberdefense.[[60]](#footnote-60) Information databases and national awareness months hosted by government or private entities help to boost awareness at the grass roots level.[[61]](#footnote-61) These programs often focus on educating individual users and smaller companies about how to protect their information and systems from cyber crimes such as identity theft and hacking. In most cases, illegal access to the computer system is only a vital first step, and hacking of individual computers or systems can be a precursor to further crimes affecting national security, such as data espionage or denial of service attacks. When carried out against vital national resources or government organs, these “crimes” may be more appropriately characterized as cyber attacks or warfare. Hackers already attempt to infiltrate governments, private businesses and national defense systems on a regular basis, with notable success.[[62]](#footnote-62) Data espionage, or the accessing of sensitive information, can be accomplished through both technical means as well as “social engineering,” a tactic which relies on human interaction to trick people into providing access to otherwise secure systems.[[63]](#footnote-63) Therefore, public education about the use of both social engineering and technical methods, such as leaving infected thumb-drives in public places, can help to protect national resources.[[64]](#footnote-64)

* 1. **Less connected and developing countries**

Although many countries rely heavily on ICTs and the Internet for critical infrastructure and services, other populations are not as dependent or connected, instead using national intranets or resources other than ICTs altogether. However, even these countries appear to be increasing their online capabilities, although such advancements may be limited to military and government uses.[[65]](#footnote-65) Countries that moved online later may face less vulnerability, as their integral government systems share fewer connections with the rest of cyberspace.[[66]](#footnote-66) But even developing countries that do not yet possess the infrastructure to enjoy the full range of benefits made possible by ICTs still depend on the Internet and other mobile and digital technologies for some of their basic needs.[[67]](#footnote-67) Thus, they too have a stake in the future of cybersecurity.

**2. Recent International Responses**

Far fewer international efforts to address the threat of cyberwar exist today than national strategies, although some attempts at multilateral initiatives have been made. Bilateral approaches have also been ventured, but these fall far short of a comprehensive strategy to improve cybersecurity and ensure cyberpeace since they only involve a very small fraction of the relevant players in the cyberpeace equation. Some countries have called for the creation of a treaty to limit the use of cyber weapons, while others have insisted that such a treaty is either unnecessary or premature. [[68]](#footnote-68) Though these proposals may evidence a step in the direction of international collaboration, they fall slightly short of a truly comprehensive approach and clear strategy for moving forward, one that includes all the relevant stakeholders. The following section introduces some recent international responses, although it is not an exhaustive list.

1. **United Nations Office of Drugs and Crime (UNODC) - The United Nations Congress on Crime Prevention and Criminal Justice (UNCPCJ)**

In April 2010, the Twelfth United Congress on Crime Prevention and Criminal Justice (UNCPCJ) drafted a set of declarations which included a provision calling for an intergovernmental expert group to study the problem of cybercrime and international responses to it.[[69]](#footnote-69) Accordingly, during the nineteenth session of the Commission on Crime Prevention and Criminal Justice, the related recommendation was made by its Member States, requesting that the commission establish an open-ended intergovernmental expert group to fulfil UNCPCJ’s provision.[[70]](#footnote-70) Though the Congress resulted in agreements on technical assistance and capacity building, it did not succeed in completely producing a consensus on the preparation of a new treaty for addressing cybersecurity issues.[[71]](#footnote-71)

1. **United Nations Economic and Social Council (ECOSOC)**

The UN Economic and Social Council (ECOSOC) opened its 2010 session with a briefing on the challenges of cybersecurity, as well as the threats posed and opportunities provided by ever-expanding use of the Internet. Among other things, the Council emphasized the need for international initiatives which would provide for information exchange, best practices, training and research. In addition, panelists stated that the United Nations must “deliver as one” on the issue, which must increase not only cooperation between countries, but also collaboration between states and the private sector to ensure cybersecurity.[[72]](#footnote-72) They cautioned that the international scope and dire consequences of an actual cyberwar require a coordinated response; ad hoc solutions and defense strengthening are now inadequate strategies.[[73]](#footnote-73)

1. **North Atlantic Treaty Organization (NATO)**

NATO implemented its own policy on cyber defense in 2008 in order to protect its technological resources and those of its member countries.[[74]](#footnote-74) As part of the policy, the alliance created a Cyber Defense Management Authority, a Computer Incidence Response Capability, which provides for the dispatch of Rapid Reinforcement Teams to individual member countries, and a Cooperative Cyber Defense Center for Excellence.[[75]](#footnote-75) Located in Estonia, the Center houses experts who conduct research and training in cybersecurity. Its sponsoring nations include Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic and Spain.[[76]](#footnote-76)

In addition, NATO has also hosted cyber defense exercises, in which teams from member states attempt to defend virtual computer networks from cyber attacks. Such exercises are intended to increase understanding of the international cyber environment and enhance international cooperation for handling technical incidents.[[77]](#footnote-77) NATO has also signed memoranda of understanding related to cybersecurity with Estonia, the United States, the United Kingdom, Turkey and Slovakia.[[78]](#footnote-78)

1. **Council of Europe – Budapest Convention on Cybercrime**

The Council of Europe Convention on Cybercrime[[79]](#footnote-79) addresses certain cybercrimes by providing model legal provisions which countries can adopt and adapt to their specific needs. While the convention provides some legal solutions to crimes like illegal access (hacking) and interception, it does not address some of the most threatening kinds of cyber incursions, such as data espionage and sabotage. And although the convention helps to foster international cooperation by criminalizing basic cybercrimes, its prescriptive power is limited by its drafter’s attempt not to contravene other potentially conflicting national legislation. Significant cultural and legal differences make the establishment of a unified law slow, if not altogether impossible, under this approach.[[80]](#footnote-80) The convention’s influence is further limited by the fact that only thirty countries have ratified the treaty since its opening for signature in November 2001, with only one of those countries hailing from outside of Europe.[[81]](#footnote-81)

Legal provisions like those set forth in the convention are one way to address some of the threats to national and international cybersecurity. However, the provisions in the convention are limited in scope and also fail to directly address the issue of cyberwar between countries, focusing instead on crimes that occur on a more localized level. While the threat of sanctions may deter some aspiring cyber criminals, this kind of legislation will likely have no effect on attackers who feel confident they can risk detection, identification or prosecution, and nor will it deter military outfits who feel compelled by the necessity of national security.

1. **Bilateral Agreements on Cybersecurity**

Individual states are also trying to build relationships with other countries in regard to cybersecurity. For example, the government of India’s Ministry of Communications and Information Technology has pursued collaborations in the form of memoranda of understanding or other development and information sharing endeavors with many different countries. For example, India and South Korea signed a joint statement for bilateral cooperation in Information Technology (IT) in 2004 and India’s Computer Emergency Response Team also signed a memorandum of understanding with Korea’s National Cybersecurity Center to establish formal collaboration in, among other areas, cybersecurity.[[82]](#footnote-82) India also has a number of other bilateral understandings related to IT generally and a few focusing specifically on cybersecurity and cyber crime.[[83]](#footnote-83)

Morocco and Malaysia also signed a memorandum of understanding on cybersecurity during the Regional Cybersecurity Conference in Morocco earlier this year.[[84]](#footnote-84) The memorandum created a cooperative relationship between the two countries’ cybersecurity ministries, covering areas including critical information infrastructure protection, cybersecurity frameworks development, capacity building, training and awareness. While these kinds of collaborations may improve a country’s cybersecurity, they are not enough to protect any one country from a global cyberwar. Therefore, a more comprehensive, global structure related to cybersecurity is needed to ensure peace for all nations.

1. **International Telecommunication Union (ITU-T Study Group 17) - Global Standards**

To address the growing issue of cybersecurity, in relation to smart grids in particular, ITU has established a Smart Grid focus group that will collect and document information and concepts that would be helpful for developing Recommendations to support Smart Grids from a telecommunication perspective.[[85]](#footnote-85) Focus groups are an ITU instrument that augments the agency’s Study Group work programme by providing an alternative working environment for the quick development of specifications in their chosen area.[[86]](#footnote-86) Focus groups are now widely used to address industry needs as they emerge, making them ideal for rapidly changing and developing technologies like Smart Grids. The Smart Grid focus group (FG Smart) consists of representatives from different member states and will collaborate with worldwide smart grid communities (e.g., research institutes, forums, academia). In achieving its objective of providing recommendations for smart grid standards, the focus group will maintain a living list of standards bodies dealing with smart grid, collect visions and value propositions for the smart grid, provide terminology and taxonomy necessary to support smart grid, gather new ideas relevant to and identify potential study areas to support smart grid, and identify the potential impact of standards development for issue areas such as security, privacy and interoperability.[[87]](#footnote-87) All of these activities will provide a comprehensive and multi-faceted approach to the quickly evolving and increasing cybersecurity challenges related to Smart Grids.

Furthermore, through its connection with ITU Telecommunication Standardization Sector (ITU-T), one of the most well recognized standards-setting organizations for telecommunications, the focus group will be able to serve as a unifying and reliable source of information and guidance, backed by a reputation for quality, consensus-based standards. The relationship with ITU-T also creates an environment conducive to the progression, if desirable, of the products of the Focus Group, through the Study Group as ITU-T Recommendations, Supplements, Manuals, etc. As part of ITU-T, the Focus Group will be able to achieve greater acceptance of its specifications in many worldwide markets, in particular in developing countries and in the regions other than the ones with more active participation in the particular forum.

1. **International Collaborations** 
   * 1. **Non-viability of deterrence**

With every new domain come new challenges. Just as the theaters of land, sea, air and space have presented questions of allocation, efficient use and conflict resolution in the past and ongoing today, so too cyberspace creates new obstacles and quandaries. Because of the unique characteristics and challenges presented by cyberwarfare, tried and true peace-keeping strategies of the past may no longer prove effective. Today, cybersecurity affects every connected person and, because of the growing reliance on ICTs for basic societal infrastructure, it now affects even those who are not connected. Attacks against information infrastructure and Internet services now have potential to harm society in new and critical ways.

Deterrence has long been a favored approach for maintaining peace and security among nations in the face of weapons that could cause massive destruction. But the efficacy of deterrence depends on certain circumstances and assumptions, many of which do not apply in the case of cyberspace.[[88]](#footnote-88) Deterrence generally requires four key elements: attribution (knowing who attacked you); location (knowing where a strike originated); response (being able to respond, even if attacked first); and transparency (the enemy’s knowledge of your capability and intent to respond with massive force).[[89]](#footnote-89) Cyberspace and cyberwar introduce new problems that undermine the basic assumption that these four elements exist when countries build their military defensive arsenals. ICTs increase the ways in which an attacker can mask his or her identity and location; attackers can use proxies or services like public Internet terminals, wireless networks and prepaid mobile services that do not require authentication. Encryption technology, which is a key technical solution to ensuring confidentiality, integrity and availability, can also be used to mask identities or at least slow the progress of an investigation into the origin of a cyber attack. Technical processes and policies that limit Internet traffic data retention also contribute to this attribution and location problem.

The risk of retaliating against the wrong target, as well as uncertainty surrounding the collateral damage of a cyber counterstrike—which could easily damage an ally or neutral party, further frustrate states’ ability to respond to an attack.[[90]](#footnote-90) If attackers believe they can remain undetected or do not believe their victims would respond with military force for fear of straying from international norms, then a retaliatory threat holds very little power. By responding with force to a cyber attack that did not use conventional military force and was intended to exploit more than destroy, a retaliating victim risks the international community interpreting their action as an aggressive and unwarranted act.[[91]](#footnote-91) Relying on a strategy of deterrence also encourages countries to engage in threatening postures towards each other and invent new retaliatory threats across different domains to compensate for possible asymmetries, frustrating the benefits of further integration and increasing tensions between nations.[[92]](#footnote-92) In all of these ways, the fundamental characteristics of cyberspace undermine the efficacy of deterrence as an approach to cyber peace.

The very framework of existing legal approaches may no longer be adequate for managing the risks related to cybersecurity. For example, under existing international law as set forth in Article 51 of the UN Charter, a state can legitimately act in its own self-defense when confronted with an armed attack. In the context of cyberwar, this calculus of course begs further questions about when a cyber attack might be viewed as tantamount to an armed attack and then whether the attack can be attributed to a nation-state.[[93]](#footnote-93) The established doctrine of ‘state responsibility’ would seem to shed some light on the latter question; it stands for the proposition that every state must act to prevent its territory from being used for attacks on other states and, if it refuses to take preventative action, it can be held responsible for such attacks. However, as we have seen in our preliminary assessments of cyber attacks, this kind of practical question becomes infinitely difficult to answer in cyberspace – some attacks do not have a geographic source (as is the case with “botnets”), they may straddle multiple borders, originate from coalitions located in multiple jurisdictions or be carried out by a proxy who is only acting on behalf of the real perpetrator. Sometimes states themselves may not be able to detect or verify which parties are acting within their own territory. And, even if a state could identify a party acting within its geographic area, the very nature of the cyber domain makes it impossible for any one single entity to exercise complete control.[[94]](#footnote-94) Thus, not only the question of source but also of control becomes infinitely murky.

* + 1. **Necessity of an international framework**

Because existing international legal norms and instruments are not fully equipped to deal with the new challenges of cybersecurity, global discussion and collaboration is now necessary. The changing nature of technology itself – with its increasing overlaps between national jurisdictions and their ICTs, online resources and systems – makes the adoption of a new set of strategies, as well as international cooperation, even more critical for ensuring cyberpeace.[[95]](#footnote-95)

Cyber attacks can originate and strike anywhere around the globe, making these threats inherently international in scope and requiring international cooperation, investigative assistance, and common substantive and procedural provisions to adequately address them. Moreover, international cooperation is already widely recognized as one of the key requirements of ensuring global cybersecurity. In 2003 and 2005, nations at the World Summit on the Information Society (WSIS) agreed on the necessity of effective and efficient tools at both the national and international levels to promote international cooperation on cybersecurity.[[96]](#footnote-96) This international collaboration should be motivated not only by a mutual desire for peace, but by each country’s enlightened self-interest. Every country is now critically dependent on technology for commerce, finance, healthcare, emergency services, food distribution and more. Loss of vital networks would quickly cripple any nation—and none is immune to cyberattack.

The pre-eminence of ICTs and the interconnectedness of developing technologies are shaping a new world order, one that calls for collaboration on new issues to ensure stability. It is important that countries harmonize their legal frameworks to combat cybercrime and facilitate dynamic, multi-faceted international cooperation. In addition to international cooperation, some groups have already called for the promulgation of international standards and cyber norms as a way of improving international cybersecurity.[[97]](#footnote-97) States should work to create a common legal and regulatory framework, and to establish a system for the regular updating of these laws to address the changing nature of security threats. An effective strategy for cyberpeace must be flexible and adaptable enough to manage and respond to the fast-pace of technological advancement, ICT growth and their attendant security challenges. Countries must also agree on procedures and approaches for tracing points of origin and identities in order to address anonymous cyber attacks and the international entanglements they threaten to create. Proposals for an international agreement requiring every country to police its own cyberspace attempt to address the problem of attribution; tying responsibility to geographic origin might sidestep the messy process of identifying exactly who orchestrated a cyberattack.[[98]](#footnote-98) However, these proposals leave unresolved the problems of identifying proxies and of tracing an attack to a geographic location—the correct location. Given the shortcomings of traditional and existing approaches to international security, it is clear that the global community must embrace a new strategy for addressing the challenges of cybersecurity and ensuring a lasting cyber peace.

1. **Proposals for International Principles of Cyberpeace**

In promulgating guiding principles for cyberpeace, we must focus on the distinctive characteristics of cyberspace and the challenges most salient to these features. However, though cybersecurity presents unique challenges, we can still draw from other undertakings aimed at combating similarly transnational threats, such as the Convention Against Transnational Organized Crime, to inform our approach. Like transnational organized crime, cyber attacks span national boundaries and operate through complex networks that parallel or overlay peaceful and productive systems. The Convention illustrates a shared understanding that these pervasive, transnational problems must be addressed by close international cooperation and that they require the adoption of new frameworks, mutual legal and development assistance, information sharing and law enforcement cooperation.[[99]](#footnote-99)

Well-established legal doctrine and internationally endorsed norms support certain necessary elements of a plan for cyberpeace. In particular, Article 19 of the Universal Declaration of Human Rights establishes the right to freedom of opinion and expression, which includes the freedom to seek, receive and impart information and ideas through any media and regardless of frontiers.[[100]](#footnote-100) In its 2003 Geneva Declaration of Principles, the World Summit on the Information Society (WSIS) reaffirmed the notion that freedom to communicate is an essential foundation of the Information Society.[[101]](#footnote-101) The Declaration further highlights the role of communication as a fundamental social process and a basic human need that serves as the foundation of all social organization. Accordingly, all people should have equitable access to information and communication technologies. The United Nations has articulated its commitment to ensuring this access to everyone and to fully harnessing the potential of the digital revolution towards this end.[[102]](#footnote-102)

Although the differences between nuclear materials and ICTs are numerous, several key similarities make international collaborations to ensure nuclear peace instructive to a strategy for cyberpeace. Like cyberspace and ICTs, nuclear energy and technology have a number of peaceful as well as military uses, they have the ability to create devastating damage if used in an attack and they could be used against any country but all countries would feel the effect of such an attack.[[103]](#footnote-103) Understanding the inherently global nature of the threat of nuclear attacks, the international community has sought a multilateral collaborative strategy that involves the creation of a common approach and a shared commitment to nuclear security.[[104]](#footnote-104) Treaties like the Non-Proliferation of Nuclear Weapons Treaty (NPT) illustrate an effective approach to the challenge of preserving peaceful uses of a potentially devastating material that has the ability to cross national boundaries. The NPT assigns responsibility for materials based on territorial jurisdiction or activities “carried out under [a state’s] control anywhere.”[[105]](#footnote-105) Echoing this approach, forty-seven nations renewed their commitment to secure nuclear materials under their control, to continue to improve security as conditions change and to exchange best practices and practical solutions for security at the 2010 Nuclear Security Summit.[[106]](#footnote-106)

The NPT also emphasizes the benefits of peaceful applications of nuclear technology and the importance of making these benefits available to all states, including developing countries.[[107]](#footnote-107) The treaty stresses the importance of international cooperation, of all states, including the exchange of information and materials to contribute to the further development of peaceful applications of atomic energy.[[108]](#footnote-108) Furthermore, Article 3 of the NPT binds signatories to certain safeguards that are intended to prevent the diversion of nuclear energy from peaceful uses to nuclear weapons or other destructive uses.[[109]](#footnote-109) The International Atomic Energy Agency, recognized for its experience, expertise and ability to facilitate discussion in a neutral forum, is charged with overseeing the negotiation and conclusion of an agreement among states which will set forth such a safeguard system.[[110]](#footnote-110)

Other relevant collaborations to ensure nuclear peace include the Global Initiative to Combat Nuclear Terrorism, an international partnership of countries committed to working individually and together to implement a set of shared nuclear security principles.[[111]](#footnote-111) These principles include: developing and improving accounting, control and security measures for nuclear substances and civilian nuclear facilities, improving member state detection and control capabilities, preventing safe havens for terrorists, improving member response, mitigation and investigation capabilities in case of attack and promoting information sharing.[[112]](#footnote-112)

International efforts to ensure peace in other new and seemingly limitless realms also strongly promote broad international cooperation. For example, the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space includes among its guiding principles the proposition that all states should pursue cooperation and mutual assistance in the exploration and use of outer space.[[113]](#footnote-113)

Recognizing the growing risk of a cyber attack that could originate anywhere and affect every nation, the ITU proposes five guiding principles for establishing and protecting peace in the emerging cyber world. These principles embody and advance the values and culture of the International Telecommunication Union, illustrated throughout its long history as a leader in international standard-setting and regulation. ITU’s authoritative International Telecommunication Regulations (ITRs) provide just one example of this tradition of promoting harmonious development, efficient operation and universal access in international telecommunications and technology. The ITRs were created as a new regulatory framework to address emerging issues and challenges accompanying the new landscape in telecommunications materializing in the late 1980s.[[114]](#footnote-114) They were crafted to promote efficiency and development within the context of collaboration, cooperation and equal access, thus exemplifying the ITU tradition. They also reflect the agency’s focus on protecting the right to communicate while also avoiding harm to facilities.

ITU’s five principles for cyberpeace similarly incorporate these core values while establishing specific actions and obligation that will ensure peace and stability in cyberspace. These principles are:

* Every government should commit itself to giving its people access to communications
* Every government will commit itself to protecting its people in cyberspace
* Every country will commit itself not to harbour terrorists/criminals in its own territories
* Every country should commit itself not to be the first to launch a cyber attack on other countries. (similar to the nuclear treaty)
* Every country must commit itself to collaborate with each other within an international framework of co-operation to ensure that there is peace in cyberspace

1. **ITU’s Global Cybersecurity Agenda (GCA)**

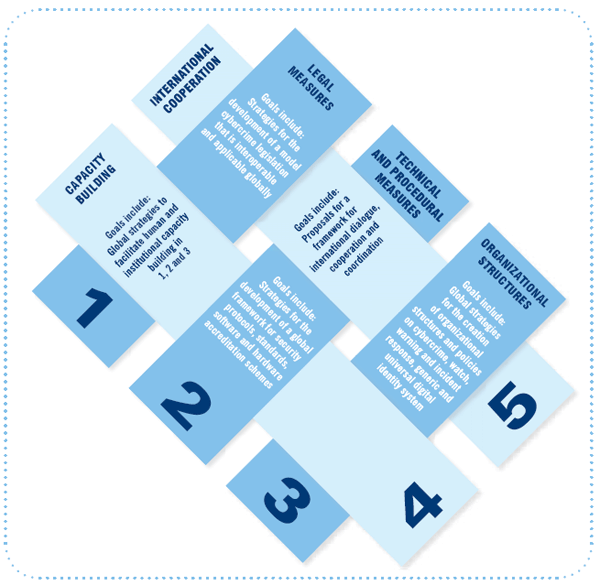
ITU provides a unique global forum for discussing cybersecurity. The agency has played a major role in telecommunications, information security and standards setting in different capacities since its founding in 1865, nearly 145 years ago. ITU understands that the scale and nature of the cybersecurity challenge requires coordinated multi-stakeholder action and it is accordingly working towards that goal. In particular, ITU is currently promoting cybersecurity through a range of activities related to standardization and technical assistance to developing countries tailored to their specific needs. In recognition of its long-standing experience, capacity and expertise, world leaders and governments appointed ITU as the sole facilitator of the WSIS Action Line C5, “[Building confidence and security in the use of ICTs.](http://www.itu.int/wsis/docs2/tunis/off/6rev1.html)”[[115]](#footnote-115) Thus, heads of states and government and other global leaders participating in WSIS as well as ITU Member States have entrusted ITU to lead the way by taking concrete steps towards curbing the threats and insecurities related to the information society. Following this appointment, ITU Plenipotentiary Resolution 140 (Rev. Antalya 2006), addressing ITU’s role in implementing the WSIS outcomes, instructed the ITU Secretary General to take all the necessary measures for ITU to fulfill its lead facilitating role in the WSIS implementation process, as a moderator for implementing WSIS Action Line C5.

Accordingly, in May 2007, ITU Secretary-General, Dr. Hamadoun I. Touré, launched [the Global Cybersecurity Agenda (GCA)](http://www.itu.int/osg/csd/cybersecurity/gca/index.html) to provide a framework within which states and other entities can coordinate an international response to the growing challenges to cybersecurity. The GCA is based on international cooperation and strives to engage all relevant stakeholders in a concerted effort to build confidence and security in the information society. The GCA is built upon five strategic pillars and made up of seven strategic goals. These goals include:

1. Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures;
2. Elaboration of global strategies for the creation of appropriate national and regional organizational structure and policies on cybercrime;
3. Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for hardware and software applications and systems;’
4. Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives;
5. Development of global strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structure to ensure the recognition of digital credentials across geographical boundaries;
6. Development of a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors and in all the above mentioned areas; and
7. Proposals on a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above mentioned areas.

In order to achieve these goals, the GCA focuses on five pillars to guide its areas of activity. These pillars are:

1. **Legal Measures**

Organized cybercrime has been on the rise because the Internet has proved a low risk, lucrative business arena. This is due to the fact that loopholes in national and regional legislation still remain, even making it difficult to effectively track down criminals. Within the GCA structure, this pillar seeks to elaborate strategies for the development of model globally applicable and interoperable cybercrime legislation. Particularly with its various cybercrime legislation resources, ITU is assisting Member States in understanding the legal aspects of cybersecurity in order to harmonize their legal frameworks.

1. **Technical and Procedural Measures**

This pillar focuses on measures for addressing vulnerabilities in software products, aiming to devise globally acceptable accreditation schemes, protocols and standards. ITU, and specifically ITU’s Standardization Sector (ITU-T) and Radiocommunication Sector (ITU-R), holds a unique position in the file of ICT standardizations and also plays a vital role in addressing security vulnerabilities in protocols. In order to identify cyberthreats and countermeasures to mitigate risks, ITU is working on secure communication services review enhancements to security specifications for mobile end-to-end data communications and considers security requirements for web services and application protocols. ITU’s focus and study groups, such as the recently formed Smart Grid focus group, provide effective mechanisms for accomplishing these goals.

1. **Organizational Structures**

The world has experienced that watch and warning systems and incident response are essential when it comes to responding to cyber attacks, as is the free flow of information, collaboration and cooperation within and between national organizational structures. This pillar, therefore, aims to create organizational structures and strategies to help prevent, detect and respond to attacks against critical information infrastructures. In this regard, ITU is working with Member States to identify their specific cybersecurity needs and assist them in establishing National Computer Incident Response Teams (CIRTs). Also, as part of ITU’s collaboration with the International Multilateral Partnership Against Cyber Threats (IMPACT), the Global Response Centre (GRC) plays a pivotal role in realizing the GCA objectives.

ITU and IMPACT formally entered into a Memorandum of Understanding in which IMPACT’s state-of-the-art headquarters in Cyberjaya, Malaysia, has effectively become the physical home of the GCA. This collaboration is providing ITU’s 191 Member States with the expertise, facilities and resources to effectively address the world’s most serious cyber-threats. The close synergies between the five work areas of the GCA and the services and infrastructure provided by IMPACT made this partnership a logical step in the global fight against cyber threats. Around sixty countries have already joined the collaboration.[[116]](#footnote-116)

IMPACT provides emergency response resources to facilitate identification of cyber threats and sharing of resources to assist member states.[[117]](#footnote-117) The Global Response Centre (GRC) is equipped with a crisis room, state-of-the-art IT and communications equipment, a fully-functional always-on Security Operations Centre, fully-redundant secure data centre, facilities for shift workers, on-site broadcasting centre and VIP viewing gallery. The GRC plays a pivotal role in realising ITU GCA’s objective of putting technical measures in place to combat new and evolving cyber-threats.

The two prime highlights of GRC are NEWS (Network Early Warning System) and ESCAPE (Electronically Secure Collaboration Application Platform for Experts). The NEWS program helps member countries identify cyber threats early on and provide critical guidance on what measures to take to mitigate them. The ESCAPE program is one of the specialized tools and systems to which Members States will have access. ESCAPE is an electronic tool that enables authorized cyber-experts across different countries to pool resources and collaborate with each other remotely, yet within a secure and trusted environment. By pooling resources and expertise from many different countries on short notice, ESCAPE will enable individual nations and the global community to respond immediately to cyber-threats, especially during crisis situations.

Not only are the objectives and resources provided by this collaboration in line with the five pillars of the GCA, they are also closely aligned with the proposed principles of cyberpeace. The resources made available to member states through IMPACT will assist each government in protecting its own people from cyber attack, thus guaranteeing their continued access to communications via the Internet and other ICTs. By joining IMPACT and participating in resource-sharing and discussions with other member states, each state will also be actively pursuing in the fifth principle – the commitment to collaborate within an international framework towards ensuring cyberpeace. In addition, IMPACT also offers scholarship grants to eligible developing country member states for training courses that will focus on building a pool of resources and acquired knowledge that trainees can later share with others to build national capacity and expertise in cybersecurity. These scholarships will improve each country’s ability to secure its own ICT resources and also to ensure access to its own people.

1. **Capacity Building**

Within the GCA framework, this pillar seeks to elaborate strategies for enhancing knowledge and expertise to boost cybersecurity on the national policy agenda. Capacity building needs to be promoted in order to develop a sustainable and proactive culture of cybersecurity. It is because understanding and awareness of the potential dangers are critical if the end-user is to benefit from ICTs safely. In particular, in line with ITU mandates to assist Member States in developing cybersecurity capacity, ITU works to facilitate the implementation and deployment of cybersecurity capabilities, such as the ITU National Cybersecurity Guide, the ITU Cybercrime Resources and the ITU Botnet Mitigation Toolkit.

1. **International Cooperation**

Cybersecurity is as global and far-reaching as the Internet. Therefore, the fifth pillar of GCA focuses on strategies for international cooperation, dialogue and coordination. The IMPACT collaboration represents substantial progress in this direction, providing a platform for member states and third parties to discuss policy and share information. This action directly promotes ITU’s mandate from a broad range of member states under the WSIS Action Line C5. The WSIS Declaration of Principles state that strengthening the trust framework, including information and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. In order to achieve this, a global culture of cybersecurity needs to be actively promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. The IMPACT collaboration, in addition to ITU’s ITRs and focus groups, strengthens this trust framework and works towards these goals by using a comprehensive approach and providing a meeting place for all members of the global community.

1. **Conclusion**

Though the threats accompanying cyber development and the increased dependence on ICTs are grave, the potential benefits are far more compelling. While we have seen some of the risks of cyberwar come to life already, we have also already reaped the benefits of cyberspace – and the possibilities for future benefits are infinite. As we move forward, we must proactively address the question of how we can continue increasing cyber dependence, development and integration, as well as how we can protect resources, create a stable environment for the continued flourishing of infrastructure and new technologies, and ensure lasting peace. Many existing approaches, although positive steps, fall short of the mark and may not provide the most effective solution. But there is a strong possibility that if we work together we can accomplish these goals and avoid the dire circumstance of cyber conflict. ITU is already effectively working towards this goal in a number of ways, and it wields the resources and influence required to foster the necessary multilateral support and participation.

1. *Elliot*, “Analysis on Defense and Cyberwarfare,” Infosec Island, 08.07.2010, available at: <https://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html>. [Hereinafter “Elliot”]. [↑](#footnote-ref-1)
2. *Messmer*, “Cyberattack Seen as Top Threat to Zap U.S. Power Grid,” Networkworld.com, 02.06.2010, available at: <http://www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html> (reporting that the threat of a coordinated cyber attack, which might be combined with a physical attack, is considered the most pressing “high-impact, low-frequency” threat to North American electricity supply). [Hereinafter “Messmer”]. [↑](#footnote-ref-2)
3. *Claburn*, “Under Cyberattack, Georgia Finds 'Bullet-Proof' Hosting With Google And Elsewhere,” InformationWeek.com, 12.08.2008, available at: <http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210002702>. [↑](#footnote-ref-3)
4. *Davis,* “Hackers Take Down the Most Wired Country in Europe,” Wired.com, 21.08.07, available at: <http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all>. [↑](#footnote-ref-4)
5. *Sang-Hun and Markoff*, “Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea,”NYTimes.com, 08.07.2009, available at: <http://www.nytimes.com/2009/07/09/technology/09cyber.html>; *Thornburgh*, “Hackers Launch Cyberattack on Federal Labs,” ABC News, 07.12.2007, available at: <http://abcnews.go.com/TheLaw/Technology/story?id=3966047&page=1>. [↑](#footnote-ref-5)
6. *Mylrea*. “Brazil’s Next Battlefield: Cyberspace,” Foreign Policy Journal, 15.11.2009, available at: <http://foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace>. [Hereinafter “Mylrea”]. [↑](#footnote-ref-6)
7. *Id*. [↑](#footnote-ref-7)
8. *Jacobs, Helft, Markoff.* “Google, Citing Attack, Threatens to Exit China,” NYTimes.com, 12.01.2010, available at: <http://www.nytimes.com/2010/01/13/world/asia/13beijing.html>. [↑](#footnote-ref-8)
9. *Van Buskirk*. “Denial-of-Service Attack Knocks Twitter Offline (Updated),” Wired.com, 06.08.2009, available at: <http://www.wired.com/epicenter/2009/08/twitter-apparently-down/>. [↑](#footnote-ref-9)
10. *See* *Sofaer/Goodman*, “Cyber Crime and Security – The Transnational Dimension”, in Sofaer/Goodman, “The Transnational Dimension of Cyber Crime and Terrorism,” 2001, at 14, available at: <http://media.hoover.org/documents/0817999825_1.pdf>. [↑](#footnote-ref-10)
11. In 1997, hackers attacked the Worcester Airport in the U.S., disabling phone services to the airport tower and shutting down the control system managing the runway lights. “Critical Infrastructure Protection, Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain,” September 2007, GAO-07-1036, available at <http://www.gao.gov/new.items/d071036.pdf>. [↑](#footnote-ref-11)
12. Elliot. [↑](#footnote-ref-12)
13. *Pennell*, “Securing the Smart Grid: The Road Ahead,” at 2, NetworkSecurityEdge.com, 05.02.2010, available at: <http://www.networksecurityedge.com/content/securing-smart-grid-road-ahead>. [↑](#footnote-ref-13)
14. Elliot. [↑](#footnote-ref-14)
15. *Coleman*, “Iranian Cyberwarfare Threat Assessment,” Defensetech.org, 23.09.2008, available at: <http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment/>. [Hereinafter “Iran”]. [↑](#footnote-ref-15)
16. “Smart Grid,” U.S. Department of Energy, available at: http://www.oe.energy.gov/smartgrid.htm; “SCADA,” TopBits.com, available at: <http://www.tech-faq.com/scada.html>. [↑](#footnote-ref-16)
17. SCADA,” TopBits.com, available at: http://www.tech-faq.com/scada.html. [↑](#footnote-ref-17)
18. *Fehrenbacher*, “10 Things to Know About Smart Grid Security,” 09.10.2009, Earth2Tech, available at: <http://earth2tech.com/2009/10/09/10-things-to-know-about-smart-grid-security/>. [Hereinafter “Fehrenbacher”]. [↑](#footnote-ref-18)
19. *Id*. [↑](#footnote-ref-19)
20. “SCADA Security and Terrorism: We’re Not Crying Wolf,” at 26, BlackHat, available at: <http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf>. [↑](#footnote-ref-20)
21. *Gorman*. “Electricity Grid in U.S. Penetrated By Spies,” WSJ.com, 08.04.2010, available at: http://online.wsj.com/article/NA\_WSJ\_PUB:SB123914805204099085.html. [↑](#footnote-ref-21)
22. *Messmer*. “’Cyberwar’ author: U.S. needs radical changes to protect against attacks,” NetworkWorld, 07.04.2010, available at: <http://www.networkworld.com/news/2010/040710-clarke-book-review.html>. [Hereinafter “Radical Change”]. [↑](#footnote-ref-22)
23. *Id.* (reporting that the U.S. electric power grid already endures hundreds of thousands of probes per day); Fehrenbacher (stating that the 40 million smart meters installed globally have already seen a number of security breaches). [↑](#footnote-ref-23)
24. Messmer. [↑](#footnote-ref-24)
25. Mylrea. [↑](#footnote-ref-25)
26. “Cyberwar: War in the fifth domain,” 01.07.2010, Economist, available at: <http://www.economist.com/node/16478792>. [Hereinafter “Fifth Domain”]. [↑](#footnote-ref-26)
27. “Smart Grid: Hardware and Software Outlook,” at p.2, Zpryme, 2009, available at: http://www.zpryme.com/SmartGridInsights/2010\_Smart\_Grid\_Hardware\_Software\_Outlook\_Zpryme\_Smart\_Grid\_Insights.pdf (stating that the U.S. smart grid industry was valued at $21.4 billion in 2009 and will reach an estimated $42.8 billion by 2014); *Weisman and Smith*. “Obama Trumpets Energy Grants,” Wall Street Journal, 28.10.2009, available at: <http://online.wsj.com/article/SB125663945180609871.html> (reporting President Obama’s announcement of $3.4 billion in stimulus grants for advanced electricity grid projects). [↑](#footnote-ref-27)
28. Fifth Domain. [↑](#footnote-ref-28)
29. *See e.g.*, *id.* (stating that “the more likely use of cyber-weapons is probably not to bring about electronic apocalypse, but as tools for limited warfare”). [↑](#footnote-ref-29)
30. *Id.* [↑](#footnote-ref-30)
31. CERT Research 2006 Annual Report, 7 et seq., available at: <http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf>. [↑](#footnote-ref-31)
32. “Understanding Cybercrime: A Guide for Developing Countries,” at 72, International Telecommunication Union, April 2009, available at <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>. [Hereinafter “Understanding”]. [↑](#footnote-ref-32)
33. *Gurmeet Kanwal*, “China’s Emerging Cyber War Doctrine,” at 20, Journal of Defense Studies, 2009, available at: http://www.idsa.in/system/files/jds\_3\_3\_gkanwal\_0.pdf (discussing China’s Information Warfare and Acupuncture policy). [Hereinafter “Kanwal”]. [↑](#footnote-ref-33)
34. For example, South Africa only recently (February 2010) announced its intention to begin to formulate a national, coordinated cybersecurity policy. “Notice of Intention to Make South African Cybersecurity Policy,” Republic of South Africa Government Gazette No. 32963, 19.02.2010, available at: <http://www.pmg.org.za/files/docs/100219cybersecurity.pdf>. [↑](#footnote-ref-34)
35. Elliot; “Cyberwar: Sabotaging the System – 60 Minutes – CBS News,” 08.11.2009, available at <http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml> (reporting that the U.S. Congress has allocated $17 billion for cybersecurity offensive and defensive initiatives). [↑](#footnote-ref-35)
36. *Deshel*, “Israel Adds Cyber-Attack to IDF,” Military.com, 10.02.2010, available at: <http://www.military.com/features/0,15240,210486,00.html>. [Hereinafter “Deshel”]. [↑](#footnote-ref-36)
37. *Coleman*, “Russia’s Cyber Forces,” DefenseTech.org, 27.05.2008, available at <http://defensetech.org/2008/05/27/russias-cyber-forces/>. [↑](#footnote-ref-37)
38. *Asmolov*, “Russia: New Military Doctrine and Information Security,” Global Voices in English, 23.02.2010, available at: <http://globalvoicesonline.org/2010/02/23/russian-military-doctrine/> (describing Russia’s updated military doctrine, which classifies information warfare as a form of military aggression). [↑](#footnote-ref-38)
39. *See, e.g.,* *Biddle*, “AFP: Huge leak of secret files sows new Afghan war doubts,” 27.07.2010, available at: http://www.google.com/hostednews/afp/article/ALeqM5gZkjOIqwM0xJDr0u5fPrc5rxdEQg. [↑](#footnote-ref-39)
40. “Cyberwarfare,” CRS Report for Congress, Updated 19.06.2001, available at <http://www.au.af.mil/au/awc/awcgate/crs/rl30735.pdf> (quoting a Russian military official who ruled out the possibility of information warfare being classified as non-military); *see also* *Beaumont*, ”US appoints first cyberwarfare general,” Guardian.co.uk, 23.05.2010, available at <http://www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general/> (reporting that the United States has also indicated it might consider using conventional military tactics to respond to cyber attacks) [Hereinafter “Cyber General”]. [↑](#footnote-ref-40)
41. “Remarks by the President on Securing Our Nation’s Cyber Infrastructure,” Whitehouse.gov, available at <http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure> (stating that that the country’s digital infrastructure would now be viewed as a “strategic national asset” and that its protection would be a “national security priority”). [↑](#footnote-ref-41)
42. Iran (estimating Iran’s cyberwarfare budget at around $76 million USD). [↑](#footnote-ref-42)
43. Kanwal at 16. [↑](#footnote-ref-43)
44. Cyberwarfare: An Analysis of the Means and Motivations of Selected Nation States, at 2, available at <http://www.ists.dartmouth.edu/docs/execsum.pdf>. [Hereinafter “Selected Nations”]. [↑](#footnote-ref-44)
45. *See, e.g., Westcott*, “UK Seeks Next Generation of Cybersecurity Specialists,” BBC News, 26.07.2010, available at: <http://www.bbc.co.uk/news/technology-10742588>. [↑](#footnote-ref-45)
46. Kanwal at 20. [↑](#footnote-ref-46)
47. *Corera*, “Cyber-security strategy launched,” BBC News, 25.06.2009, available at: <http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm?ad=1> [Hereinafter “Corera”]; *Gjelten*, “Cyberwarrior Shortage Threatens U.S. Security,” National Public Radio, 19.07.2010, available at: <http://www.npr.org/templates/story/story.php?storyId=128574055>. [↑](#footnote-ref-47)
48. Deshel. [↑](#footnote-ref-48)
49. Kanwal at 20. [↑](#footnote-ref-49)
50. Some countries have disclosed their massive personnel shifts. *See* Cyber General (stating that the United States announced reassignment of 30,000 troops to cyber combat). However, information on many countries’ strategies is less accessible. *See* *McMillan*, “Black Hat Talk on China’s ‘Cyber Army’ Pulled After Pressure,” InfoWorld.com, 15.07.2010, available at: http://www.infoworld.com/print/130362. [↑](#footnote-ref-50)
51. Deshel*.* [↑](#footnote-ref-51)
52. For example, the United States announced the creation of a new cyber military unit in 2009. Cyber General. The United Kingdom also recently announced the creation of a cybersecurity operations center as part of its cybersecurity strategy. Corera. [↑](#footnote-ref-52)
53. *See* “U.S. Cyber Command Fact Sheet,” U.S. Department of Defense, available at <http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf> [↑](#footnote-ref-53)
54. *Gorman*, “U.S. Backs Talks on Cyberwarfare,” WSJ.com, 04.06.2010, available at: <http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html> (noting that 90% of U.S. military power is provided by the private sector, according to U.S. military officials). [Hereinafter “Gorman”]. [↑](#footnote-ref-54)
55. Kanwal at 16. [↑](#footnote-ref-55)
56. Kanwal at 14. [↑](#footnote-ref-56)
57. Kanwal at 18. [↑](#footnote-ref-57)
58. Radical Change(“Because the United States is the most Internet-dependent and automated . . . it’s also the most vulnerable to cyberattack.”). [↑](#footnote-ref-58)
59. Kanwal at 18; CRS Report for Congress: Cyberwarfare, at 11, updated June 19, 2001, available at: <http://www.au.af.mil/au/awc/awcgate/crs/rl30735.pdf> . [↑](#footnote-ref-59)
60. *E.g.*, Selected Nations at 5 (recommending systematic and sustained efforts to change the way the U.S. populace views network security in order to improve national cybersecurity). [↑](#footnote-ref-60)
61. For example, Mauritius’ National Computer Board, under the purview of its Ministry of Information and Communication Technology, oversees a Cybersecurity Awareness Portal, available at http://www.gov.mu/portal/sites/ncbnew/main.jsp, and the United States observes a National Cybersecurity Awareness Month. Public-private partnerships, like the U.S. National Cybersecurity Alliance, also educate users and administrators of digital infrastructure on how to build resilient systems and protective mechanisms. “About Us,” The National Cybersecurity Alliance, available at: http://www.staysafeonline.org/content/about-us. [↑](#footnote-ref-61)
62. *See, e.g.*, Understanding at 20 (listing famous targets of various hacking attacks, including the Pentagon, the German government, Google, Ebay and NASA). [↑](#footnote-ref-62)
63. *See* *id.* at 23-24. [↑](#footnote-ref-63)
64. For example, U.S. Central Command was infiltrated by an infected thumb-drive in 2008. *See* Fifth Domain. [↑](#footnote-ref-64)
65. *Williams*, “North Korea Moves Quietly Onto the Internet,” Computerworld.com, 10.06.2010, available at: http://www.computerworld.com/s/article/9177968/North\_Korea\_moves\_quietly\_onto\_the\_Internet. [↑](#footnote-ref-65)
66. Corera*.* [↑](#footnote-ref-66)
67. *E.g.*, “Economic and Social Council Opens General Segment of 2010 Session,” at 3, ECOSOC/6444, available at http://www.un.org/News/Press/docs/2010/ecosoc6444.doc.htm (discussing the “digital cash” or electronic money system used in African countries). [↑](#footnote-ref-67)
68. Gorman. [↑](#footnote-ref-68)
69. “Draft Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World,” Declaration 42, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 18.04.2010, available at: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6\_Rev.2/V10529031A\_CONF213\_L6\_REV2\_E.pdf. [↑](#footnote-ref-69)
70. “Report on the nineteenth session,” Economic and Social Council, Commission on Crime Prevention and Criminal Justice, available at: http://www.unodc.org/documents/commissions/CCPCJ\_session19/E2010\_30ADVANCE\_UNEDITED\_VERSION.pdf. [↑](#footnote-ref-70)
71. “Summary of outcome regarding cybercrime: 12th UN Congress on Crime Prevention and Criminal Justice,” Project on Cybercrime, 26.04.2010, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/2079\_UNCC\_cyberoutcome.pdf. [↑](#footnote-ref-71)
72. “Economic and Social Council Opens General Segment of 2010 Session,” 37th & 38th Meeting, ECOSOC/6444, available at: <http://www.un.org/News/Press/docs/2010/ecosoc6444.doc.htm>. [↑](#footnote-ref-72)
73. *Id.* (discussing the “digital cash” or electronic money system used in African countries). [↑](#footnote-ref-73)
74. “Defending Against Cyber Attacks,” NATO, <http://www.nato.int/cps/en/natolive/topics_49193.htm>. [↑](#footnote-ref-74)
75. NATO 2020, available at http://www.nato.int/cps/en/natolive/official\_texts\_63654.htm?selectedLocale=en. [↑](#footnote-ref-75)
76. Cooperative Cyber Defense Center for Excellence, available at http://www.ccdcoe.org/. [↑](#footnote-ref-76)
77. “Defence exercise to boost skills for countering cyber attacks,” NATO-News, 10.05.2010, available at: http://www.nato.int/cps/en/SID-012B6A76-D60B9579/natolive/news\_63177.htm. [↑](#footnote-ref-77)
78. “NATO and Estonia conclude agreement on cyber defense,” NATO-News, 23.04.2010, available at: www.nato.int/cps/en/natolive/news\_62894.htm. [↑](#footnote-ref-78)
79. Convention on Cybercrime CETS no.: 185, Council of Europe, available at: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>, last visited on 10.08.2010. [Hereinafter “Convention”]. [↑](#footnote-ref-79)
80. “National Security Threats in Cyberspace,” at 13, American Bar Association Standing Committee on Law and National Security and National Strategy Forum, Sept. 2009, available at: http://www.abanet.org/natsecurity/threats\_%20in\_cyberspace.pdf. [↑](#footnote-ref-80)
81. Convention. [↑](#footnote-ref-81)
82. “Bilateral Cooperation: Asia,” India Department of Information Technology, Government of India Ministry of Communications and IT, available at: http://www.mit.gov.in/content/asia. [↑](#footnote-ref-82)
83. For example, India’s collaborations with Brunei, Malaysia, France and Australia specifically focus on information security and/or cyber crime, while other relationships focus on development of resources and facilities. “Bilateral Cooperation,” India Department of Information Technology, Government of India Ministry of Communications and IT, available at: http://www.mit.gov.in/content/bilateral-cooperation. [↑](#footnote-ref-83)
84. “Malaysia and Morocco Are Now Partners in Cybersecurity,” CyberSecurity Malaysia, 24.01.10, available at http://www.cybersecurity.my/data/content\_files/44/632.pdf?.diff=1265036362. [↑](#footnote-ref-84)
85. For more information on the Focus Group, please visit http://www.itu.int/ITU-T/focusgroups/smart/. [↑](#footnote-ref-85)
86. ITU-T Focus Groups, available at: http://www.itu.int/ITU-T/focusgroups/. [↑](#footnote-ref-86)
87. Terms of Reference of ITU-T Focus Group on Smart Grid, available at: http://www.itu.int/ITU-T/focusgroups/smart/tor.html. [↑](#footnote-ref-87)
88. Radical Change (quoting former U.S. security advisor Richard Clarke as stating that, “the force that prevented nuclear war – deterrence – does not work well in cyberwar”). [↑](#footnote-ref-88)
89. *Lan, Tang and Zhang Xin*, “The View From China: Can Cyber Deterrence Work?” at 1, Global Cyber Deterrence, EastWest Institute, April 2010, available at: http://www.ewi.info/system/files/CyberDeterrenceWeb.pdf. [↑](#footnote-ref-89)
90. *Lewis, James A.,* “Cross-Domain Deterrence and Credible Threats,” Center for Strategic and International Studies, July 2010, available at: <http://csis.org/files/publication/100701_Cross_Domain_Deterrence.pdf>. [↑](#footnote-ref-90)
91. *Id*. [↑](#footnote-ref-91)
92. *Id.* [↑](#footnote-ref-92)
93. “National Security Threats in Cyberspace: A Workshop,” at 14, American Bar Association Standing Committee on Law and National Security and National Strategy Forum, 2009, available at: <http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf>. [Hereinafter “Workshop”]. [↑](#footnote-ref-93)
94. *Id.* [↑](#footnote-ref-94)
95. *Id.* [↑](#footnote-ref-95)
96. “WSIS: Tunis Agenda for the Information Society,” Paragraph 40, World Summit on the Information Society, 2005, available at: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>. [Hereinafter “Tunis Agenda”]. [↑](#footnote-ref-96)
97. Participants at a workshop including members of the American Bar Association Standing Committee on Law and National Security, the McCormick Foundation and the National Strategy Forum contemplated the formation of an international Cybersecurity Action Task Force to devise cyber norms and rules to improve cybersecurity. Workshop at 26. [↑](#footnote-ref-97)
98. *Mullins*, “’Pearl Harbor’ post struck a nerve,” NetworkWorld.com, 11.03.2010, available at: <http://www.networkworld.com/community/node/58450> (quoting former U.S. presidential security advisor Richard Clarke at a recent cybersecurity panel discussion). [↑](#footnote-ref-98)
99. Convention Against Transnational Organized Crime, United Nations Office on Drugs and Crime, 2004, available at: http://www.unodc.org/unodc/en/treaties/CTOC/index.html. [↑](#footnote-ref-99)
100. Universal Declaration of Human Rights, Article 19, U.N. G.A., Res. 217A (III), U.N. GAOR, U.N. Doc. A/810 (1948), available at: http://www.un.org/en/documents/udhr/index.shtml#a19. [↑](#footnote-ref-100)
101. Geneva Declaration of Principles, Para. 4, World Summit on the Information Society, 2003, available at: http://www.itu.int/dms\_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf. [↑](#footnote-ref-101)
102. “Ban urges greater use of digital technology to improve living conditions,” UN News Centre, 17.05.2010, available at: http://www.un.org/apps/news/story.asp?NewsID=34716. [↑](#footnote-ref-102)
103. National Statement of the United States, 2010 Nuclear Security Summit, 13.04.2010, available at: http://www.whitehouse.gov/the-press-office/nuclear-security-summit-national-statement-united-states. [↑](#footnote-ref-103)
104. *Id.* [↑](#footnote-ref-104)
105. Treaty on the Non-Proliferation of Nuclear Weapons (NPT), Art. 3, 1970, available at: <http://www.un.org/disarmament/WMD/Nuclear/pdf/NPTEnglish_Text.pdf>. [Hereinafter “NPT”]. [↑](#footnote-ref-105)
106. National Statement of the United States. [↑](#footnote-ref-106)
107. NPT at Preamble and Art. 5. [↑](#footnote-ref-107)
108. *Id.* at Preamble. [↑](#footnote-ref-108)
109. *Id.* at Art. 3. [↑](#footnote-ref-109)
110. *Id.* [↑](#footnote-ref-110)
111. “The Global Initiative to Combat Nuclear Terrorism,” U.S. Dept. of State, available at: http://www.state.gov/t/isn/c18406.htm. [↑](#footnote-ref-111)
112. “Statement of Principles,” The Global Initiative to Combat Nuclear Terrorism, U.S. Dept. of State, available at: http://www.state.gov/documents/organization/141995.pdf. [↑](#footnote-ref-112)
113. Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space (the “Outer Space Treaty”), Principle 6, 1967, available at: http://www.oosa.unvienna.org/oosa/SpaceLaw/lpos.html. [↑](#footnote-ref-113)
114. “International Telecommunication Regulations: Final Acts of the World Administrative Telegraph and Telephone Conference,” International Telecommunication Union, 1989, available at: http://www.itu.int/osg/spu/intset/itu-t/mel88/mel-88-e.pdf. [↑](#footnote-ref-114)
115. Tunis Agenda. [↑](#footnote-ref-115)
116. “International Multilateral Partnership Against Cyber Threats,” International Telecommunication Union, available at: <http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html>. [↑](#footnote-ref-116)
117. [ITU Information Letter sent to all ITU Member States on the "Deployment of Cybersecurity Capabilities - IMPACT Global Response Centre,"](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT-information-letter-sent-to-member-states-2009.pdf) available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT-information-letter-sent-to-member-states-2009.pdf. [↑](#footnote-ref-117)