An ISGP White Paper:

Cybersecurity

Introduction

The explosive growth of cyberspace, which includes the internet and interconnected information technologies such as wireless devices and cell phones, is creating unprecedented connectivity and societal benefits throughout all aspects of the global community. With this new socio-technical landscape, however, has come a raft of new vulnerabilities and threats to national security, our economic systems, and personal privacy, as well as many other fundamental aspects of modern life. All indicators point to the continued rapid growth of cyberspace that is taking all societies into uncharted areas of security, policy, and governance. Our ability to grasp the magnitude of this issue and its consequences requires analyses that link credible scientific understanding and technological options with the "actionable decisions" needed to formulate and implement practical policies. In this **White Paper**, the **Institute on Science for Global Policy** (ISGP) undertakes a preliminary examination of the issues related to ***Cybersecurity*** by summarizing the current realities, the scientific and technological (S&T) challenges and opportunities, and some of the related domestic and international policy issues facing societies and their governments.

The ISGP Approach

Many of the most significant global challenges for 21st century societies are directly related to the profound S&T achievements of our time. Success in fostering safe, secure, and prosperous societies often reflects how well societal and governmental institutions recognize the opportunities and consequences associated with existing, emerging, and "at-the-horizon" S&T and how effectively governmental policies balance short-term challenges requiring immediate attention with the need for long-term investments in transformative research and development (R&D). Unfortunately, large gaps too often exist between S&T understanding and the governmental policies that emerge from the political processes within a society.

The ISGP seeks to significantly improve the capability of governments to effectively bridge these gaps and to help shape the relevant domestic and international policies. ISGP programs use a unique format based on multiple conferences designed to address specific aspects (e.g., attribution, situational awareness, cybercrime, cyber attacks, etc.) of a broad S&T topic (i.e., ***Cybersecurity***) previously vetted as a priority with participating governments. While each ISGP program focuses on a specific S&T topic (e.g., energy, infectious diseases, food safety, or cybersecurity), the ISGP is positioned to examine several S&T topics simultaneously through parallel programs.

Each ISGP conference focuses almost exclusively on critical debates and caucuses involving highly credible, articulate scientists chosen by the ISGP and an international group of policy makers from the United States, Europe, and Asia selected by the participating governments. The ISGP selects a few (6-8) S&T experts for each conference to prepare concise, focused written documents describing their views and to participate in the critical debates led by a global group of decision makers. Emphasis remains on specific "actionable decisions" and their foreseeable consequences. Separate caucuses held during each ISGP conference provide opportunities for governmental and societal representatives to discuss next steps, both domestically and internationally.

In preparation for each conference, the ISGP staff interviews or corresponds with a wide range of globally recognized subject matter experts from academia, industry, and the non-governmental community. These discussions seek to elicit the interviewee's opinions concerning the relevant current realities, S&T challenges and opportunities, and policy options that should be considered by governments. To ensure a comprehensive understanding of these issues, the ISGP also reviews the relevant international reports, statements, and S&T publications. Taken together, these materials and information are used by the ISGP to prepare a **Strategic Roadmap** which not only summarizes all the findings, but also describes the content and structure of a series of 6-8 conferences to be convened by the ISGP on the S&T topic (e.g., ***Cybersecurity***) over a two-three year period.

The global character of the ISGP is reflected not only through the engagement of the United States, European, and Asian governments, but also in its international network of affiliated universities. Students and professors from these affiliated institutions participate in ISGP programs and are involved in real decision-making processes occurring at each ISGP conference (fundamentally a "practical policy laboratory"). ISGP programs also seek to foster public respect for the role of S&T in policy, and obviously, to help shape strategic public policies worldwide.

Cybersecurity

This **ISGP White Paper** has been developed to summarize the current scientific understanding and to identify some of the critical policy issues that make ***Cybersecurity*** an appropriate topic to be examined through a comprehensive, two-three year ISGP program. It is based on a review of some of the relevant published material and on discussions with a selected group of S&T professionals versed in cyberspace issues through their work in academic, private sector, and non-governmental settings. While these individuals were asked for their opinions, they did not author or formally endorse this **ISGP White Paper on *Cybersecurity***, which remains wholly a product of the ISGP.

In a two-three year comprehensive study, the ISGP would examine ***Cybersecurity*** using the multiple conference procedures and critical debate format described above. This would involve a much larger number of interviews with subject matter experts and policy makers chosen internationally and would lead to the preparation of a **Strategic Roadmap on *Cybersecurity*** that would be reviewed by participating governments before its implementation.

Efforts to establish strategies to secure cyber infrastructures throughout the global community must be predicated on an accurate understanding of the consequences of both our actions and our inactions. Identifying effective domestic and international policies connected to the "actionable decisions" that underlie sustainable solutions requires conscientious deliberation rooted in the credible S&T options. Such solutions will represent a mosaic of near-, mid-, and long-term approaches. Effective near-term policies must obtain international consensus and establish measurable, enforceable agreements affecting both domestic and international decisions. Mid-term policies are likely to be derived from evolutionary S&T developments. Long-term approaches are anticipated to become apparent only after R&D efforts identify revolutionary S&T advances. To formulate and implement policies without informed discussion and debate of all three types of options risks highly unpredictable experimentation with one of the most influential components of modern societies, namely rapid, global communications.

Current Realities – Overview

With the rapid development of information and communication technologies (ICT) and the full privatization of the internet almost twenty years ago has come one of the most transformational periods in human history. Cyberspace has become a functionally multifaceted infrastructure of

enormous size and scope, and it's very low cost of entry and use has allowed participation by a large fraction of mankind. At present, nearly 1.5 billion people worldwide have access to cyberspace, and with governmental support and philanthropic private sector programs such as the $100 Laptop Initiative, growth in global cyberspace usage will continue to expand. In addition to human users, there are also millions of sub-networks and technology systems interfaced with the infrastructure backbone that defines cyberspace.

Perhaps the most important single property of cyberspace is its ubiquitous presence across the public and private domains, across societal and economic sectors, from individual use to control of large systems and organizations, and its nearly seamless integration across national borders. Such scope is so unprecedented that there is difficulty in grasping its properties and measuring its behavior. In fact, wholly new mathematical theories have been developed in the last decade motivated by the need to understand cyberspace quantitatively. From a policy and governance standpoint, the ubiquitous nature of cyberspace presents fundamental challenges at the interface of public versus private sector control, and at the boundaries of local to state to national to international jurisdiction.

An even more serious and practical set of problems is the increasing misuse of cyberspace for malicious intent. These actions range in increasing severity from spamming to hacking, denial of service attacks, cybercrime, cyber-terrorism, and even attack by and on nation states for intelligence gathering or in coercive operations which approach warlike actions. These actions present serious policy and legal issues that have yet to be effectively addressed because of the absence of firm national and international frameworks that classify such events and regulate that appropriate type of national or international response. The absence of such frameworks is often at least partly due to underlying technological issues, such as an inability to exactly identify the sources or perpetrators of such attacks.

Current Realities – Threat Spectrum

As the extent of cyberspace increases, and experience is gained in exploiting its power, the level of malicious activity has risen steadily. For example, while spam was nearly unknown around the year 2000, some analyses now estimate that spam makes up nearly 90% of the emails sent globally. While spam may be more of a nuisance than a threat, a wide range of malicious activity now exists which can be far more serious. These threats are extremely diverse in their intended goals, their extent, their sophistication, and the potential damage they could inflict. They are perpetrated by a wide range of groups which include hackers, activists, disgruntled employees, industrial spies, organized crime, terrorists, and nation states. The US Government (USG) is a particularly common target of attacks of all types, and the numbers of attacks are increasing steadily. In 2005, the Department of Homeland Security (DHS) reported 4,095 attacks on the USG, while in 2007, that number had increased to 37,258.

Several organizations, both in the US and worldwide, attempt to track and classify malicious cyber activity. The United States Emergency Readiness Team (US-CERT) publishes a list of cybersecurity trends and indicators that categorize the main threat activities into unauthorized access, denial of service, malicious code, improper usage, scans and probes, and phishing. Currently, phishing accounts for the greatest number of attacks, while scans and probes are increasing rapidly. The effects of such attacks include theft of personal data, co-opting systems, the corruption of web portals, spyware, and financial scams. Hacking alone has led to the loss of billions of dollars to the private sector.

A far more important class of threats is that related to national and homeland security. While perpetrators of such attacks include political and terrorist organizations, an increasing number of nation states are developing sophisticated cyber capabilities for intelligence gathering and even offensive operations. Targets of such attacks are often sensitive military or critical infrastructure

networks or information repositories. Because such networks often coordinate or control a large number of assets or personnel, an attack on them can have far reaching effects. For example, experts fear that a well coordinated cyber attack could seriously disrupt the electric grid or transportation network serving a large region for a prolonged period. A particularly disturbing trend recently has been the use of cyberspace to augment or replace military operations. An example occurred in 2007 when Russia launched what many consider to be the world's first cyber war against Estonia, and later used cyber attacks in conjunction with its military operations against Georgia. Many such incidences of international cyber attacks have been traced to sources within China.

Current Realities – Technology Gaps

Many of the reasons behind the level of malicious activities in cyberspace can be traced to technological nuances or deficiencies. The original design of the world-wide web can make it nearly impossible to determine the exact identity or location of a specific user on the web. Moreover, because of the sheer size of the networks and the diverse activities involved, it is nearly impossible to gain situational awareness about even relatively modest areas of the web.

These characteristics severely limit the degree to which large scale coordination or response to major cyber events can be effective. As increasingly sophisticated wireless and telecommunication devices populate the web, these problems are only exacerbated. The increasing sophistication of software required to support the networks and its applications, and the commercial pressures to publicly introduce them as quickly as possible, mean that many design flaws and bugs remain unnoticed for years. These design flaws are often exploited by hacking communities. Finally, the size, sophistication, and novelty of such a global super system even challenge current scientific understanding of how to measure, model, and control the properties of the network. These challenges will require well planned, holistic research agendas designed to address the full spectrum of technology and commercialization issues in a synergetic and efficient manner.

Current Realities – Coordination and Governance

Questions about the security, control, and governance of cyberspace can generally be divided between those within the purview of the public versus those within the control of the private sector. While governments generally have many critical assets affected by cyberspace, and a statutory mission to safeguard their nation's critical infrastructures, in fact, a large portion of these infrastructures (particularly within the US) lie within the private sector. Additionally, because cyberspace extends nearly seamlessly across most international borders, global coordination and governance of cyberspace are particularly problematic. There are, therefore, significant domestic and international policy and legal issues which come into play concerning coordination and boundaries of authority in dealing with preparedness, detection, and response to malicious cyber activities. Many of these issues arise simply because cyberspace is a relatively new phenomenon without significant legal or regulatory precedence in either the public or private sectors.

Within the USG, coordination of cybersecurity activities has been an evolving issue in recent years. While the Department of Defense (DoD) probably has the most resources in this domain, their mission obviously does not include most of the domestic and private sectors. The Department of Homeland Security (DHS) has a mission to help secure domestic assets, however their resources are limited. More recently, there have been efforts to centralize coordination of cybersecurity efforts within the USG. In 2007, the DoD attempted to set up a joint service Cyber-command as part of the 8th Air Force. This effort has been disbanded. The National Security Agency (NSA) has continued to make a case that they have the most relevant expertise and assets in this area. In 2008, the Bush Administration established the

Comprehensive National Cybersecurity Initiative (CNCI) as an interagency effort to secure Federal ICT systems. However, this is a classified activity and many experts argue that its limited transparency prevents any effective engagement with the private sector. The Obama administration is currently still reviewing its plans for a comprehensive response by the Federal government, and has appointed a cyber czar who will chair the Information and Communications Infrastructure Interagency Policy Council (ICI-IPC).

Scientific Challenges and Opportunities

Many of the most important cybersecurity issues are directly related to technology. Because the technologies themselves are relatively new and very rapidly evolving, significant gaps exist in understanding their properties as well as the behavior of the large scale systems which employ them. These technological gaps in turn create significant uncertainties when creating response strategies, and development of policy and regulation. Some of the most important technology issues are listed below:

Scientific Challenges and Opportunities – Attribution

One of the most salient properties of cyberspace currently is its relative anonymity, often referred to as the attribution issue. Attribution refers to the ability to ascertain identities on the web, either of specific accounts or systems or of human users, and to attribute specific actions to them with certainty. While mechanisms do exist to identify users obeying normal guidelines and protocols, it has proven relatively easy for malicious entities to falsify identities. Methods include simple techniques such as co-opting of user accounts, to the more elaborate schemes such as operating in countries with relatively little control over their networks. The attribution issue is extremely important because it can greatly limit the ability of law enforcement to produce evidence against a specific perpetrator or for a national government to uniquely identify the source of a major cyber attack. While much research and operational methodology is invested in addressing the attribution issue, some experts have argued that only a complete re-design of the cyber networks can effectively secure them against the uncertainties of attribution.

Scientific Challenges and Opportunities – Situational Awareness

Situational awareness refers to the ability to ascertain the current state of an operational environment so that relevant courses of action can be developed. In the cyberspace domain, this implies the necessity of gathering data from computer systems, networks, and information flows, as well as systems affected by them. The sheer size of the networks (e.g. millions of nodes), however, can make this task nearly impossible. To improve this situation, better methods must be developed for real-time system diagnosis, data fusion, event correlation, information synthesis, network state visualization, and threat assessment and prediction. In some cases, this will involve not only better schemes for implementation, but fundamental advances in scientific knowledge and computer engineering.

Scientific Challenges and Opportunities – Threat Profiles

One of the principal methodologies for dealing with cyber threats is profiling. Simply stated, threat profiling attempts to deduce characteristics of potential attacks, so that they may be identified earlier, and response strategies can be developed ahead of time. From a purely technical approach, an example of threat profiling is the identification and characterization of cyber worms, and the dissemination of their profiles to computer security software so they can be identified prior to infection. However, even more sophisticated methods of threat profiling involve the categorization and identification of threat actors, their attack strategies and tools. By fusing technical indicators with a range of indicators based on attacker motives and intentions, analysts are able to categorize threat entities, engage in trend analysis and predict a course of action to counter the threat. While some aspects of sophisticated threat profiling involve

technological challenges, an understanding of the socio-behavioral and operational factors is no less important. Significant progress in defining research methodologies for predicting the sociological and human behavioral contributions leading to cyber threats is needed if effective approaches are to be developed.

Scientific Challenges and Opportunities – Analysis, Modeling and Simulation

The sheer size and complexity of cyberspace poses enormous challenges to understanding even its basic structural and behavioral properties. It has become increasingly clear that conventional analytic tools and human insight are insufficient to fully characterize cyberspace, plan operational strategies, and develop effective policies. Better analytic tools and predictive techniques must be developed. Fortunately, this need has already led to important advances in fundamental science. For example, cyberspace itself motivated much of the recent work on small-world theory and scale-free networks, arguably one of the most important advances in network theory in recent decades.

In addition to the networks themselves, it is necessary to develop better tools that integrate the socio-behavioral aspects of the human and organizational components of cyberspace. Such tools will require the continued development of advanced analytic capabilities, as well as modeling and simulations tools such as agent-based models, which can provide accurate and relevant knowledge and predictive capabilities to those engaged in operations, policy, and decision-making.

Scientific Challenges and Opportunities – Testing, Training, Experimentation, Outreach

Cyberspace is a new and complicated environment, and as with the adoption of any new technology, there are significant issues related to cultural acceptance and human behavior that influence the development of best practices. Many cybersecurity issues are related to sociological factors. Simple practices such as regularly changing passwords have been identified as having considerable positive value for cybersecurity. Collectively, these factors are generally addressed under the topic of education and training. In the US, the ICI-IPC has recently identified these topics as a near-term priority for improving the national cybersecurity posture. Additionally, more technical topic areas related to human factors include testing and experimentation. These areas address increasing the capacity for human users to test and train on new security technologies, methods, and operational doctrine. One major deficiency in current technology is that no cyber conflict experimentation environment exists with a sufficiently large number of network nodes to model large scale cybersecurity phenomena. To address this problem in the US, the Defense Advanced Research Project Agency (DARPA) is currently developing the National Cyber Range (NCR), a sophisticated test-bed environment with thousands of nodes which will be available for classified and unclassified research. More investment of this type is needed to give researchers and operators alike the technological capabilities to gain practical experience.

Scientific Challenges and Opportunities – Coordinating R&D Funding

One of the most important strategic issues underlying cybersecurity involves development and coordination of broad R&D portfolios. Such programs are intended to create the underlying scientific knowledge, technological tools, and operational insights to address the major challenges posed by cyberspace, and to do so in an effective and economically efficient manner. Because cyberspace involves so many technological and societal aspects, this goal has proven difficult to reach. An effective research portfolio must include traditional disciplines such as physics, computer science, information science, information technology (IT) engineering, systems engineering, and data sciences. Increasingly, however, it must include economics and the socio-behavioral sciences, and disciplines such as psychology, risk analysis,

and complex systems which can address the multi-disciplinary nature of cyber threats. The definition of a well balanced R&D portfolio is an ongoing issue which is made more difficult by the rapidly changing nature of the cyber landscape.

An important aspect of developing these R&D strategies is the creation of effective organizations which can define and manage them. Within the USG, the Networking and Information Technology Research and Development program (NITRD), part of the Executive Office of the President (EoP), is the interagency group which coordinates cybersecurity R&D across 13 Federal agencies and a wide range of topic areas. In 2006, the NITRD produced a plan for Federal cybersecurity R&D, which recommended funding research on topics including high-impact threats, emerging technologies, creation of metrics to assess cybersecurity, and of assessing ways of building security in from the beginning. The report also recommended strengthening partnerships between the USG and the private sector and with selected partners internationally. The plan recommended the development of a cybersecurity strategic roadmap, which has not yet been produced. The new Obama administration is currently reviewing these recommendations and has stated that it intends to make cybersecurity one of its key management priorities.

Policy Issues

While cybersecurity first became recognized as a significant technological and policy issue well over a decade ago, response by the public and private sectors has often been slow. Only relatively recently has the severity of potential threats been widely recognized, and significant national efforts been made to define response and policy frameworks. A variety of large scale studies have appeared in recent years proposing research agendas, policy frameworks, and national coordinating mechanisms. These frameworks have evolved steadily as the cybersecurity landscape has changed, and as such appear complex and sometimes even *ad hoc*. The complexity of these issues reflects the rapidly changing technological, economic, legal, and political factors that now underlie cybersecurity.

In recent years, it has become increasingly clear that cybersecurity problems cannot be solved by national governments alone. It will require a concerted effort with State and local governments, the private sector, civil society, and perhaps most importantly, international partners. Many of the most important policy and coordinating efforts are summarized below.

Policy Issues – National Organization

Because of the broad scope of cyberspace and the systems it affects, national governments must begin to take increased responsibility for addressing cyber activities which occur within their respective borders. Such responsibilities include technology deployment and economic aspects, but increasingly will include policy development, R&D, law enforcement, and even national security. Few governments currently make cybersecurity such a priority. Without significantly improving national programs that can be effectively coordinated across the international community, large portions of cyberspace will remain unregulated and thereby havens for malicious actors.

In terms of coordination within the USG, cybersecurity efforts now span the entire government, and are divided into Civilian Defense (6 Agencies), Commercial Defense (8 agencies), and Intelligence and Military Threats (7 Agencies). DHS has been designated as the lead agency in the overall development of cyber capabilities, and has particular responsibility for securing the 18 critical infrastructure sectors. The President coordinates interagency cybersecurity activities through the Assistant to the President for National Security and the Assistant to the President for Homeland Security. As mentioned previously, the CNCI was created in 2008 to coordinate Federal cyber activities, and recently the National Cybersecurity Center (NCSC) was also

created under DHS to oversee and coordinate CNCI activities. This is a significant development since it is the first time USG cybersecurity activities will be coordinated through a single office.

Several USG strategy documents have been produced over the last few years which attempt to develop high level policy frameworks for various aspects of the national cybersecurity landscape. These include the National Strategy to Secure Cyberspace (2003), Homeland Security Presidential Directive 7 (2003), parts of the National Security Strategy of 2006, the National Strategy for Homeland Security (2007), and the National Strategy for Information Sharing (2007). These documents attempt to set overarching goals for securing US cyber assets, research priorities, and also lay out responsibilities among the Agencies.

While the policy recommendations in these documents are too detailed to cover here, a few common threads run through all of them. These include:

a. the necessity of developing strong partnerships between the USG, state and local authorities, the private sector, civil society, academia, and international partners;

b. the necessity of information sharing and the coordinating mechanisms to do so, such as the Information Sharing and Analysis Centers (ISACs);

c. effective processes and organizations to evaluate threats, vulnerabilities, risks, and economic factors;

d. mechanisms to promote response, recovery, and resiliency to attacks;

e. capabilities to detect, prevent, and defeat terrorist cyber attacks;

f. the importance of funding research, development, and technology transition to provide both evolutionary and revolutionary technological solutions.

Cybersecurity R&D has similarly been the subject of several large studies and policy reports in recent years. The most notable of these include: The National Academy of Sciences *Toward a Safer and More Secure Cyberspace*; the INFOSEC Research Council's *Hard Problem List*; and the Institute for Information Infrastructure Protection's *National Cybersecurity Research and Development Challenges.* These documents provide lists of the most important technology problem areas and research disciplines which can address important cybersecurity issues, and provide an organizing framework for creating well-balanced R&D portfolios.

Other countries are now making significant efforts to coordinate cybersecurity activities and develop policy and regulation. In the 2009, the United Kingdom established within their government the Office of Cyber Security, and the Cyber Security Operations Center, and has also published a national Cyber Security Strategy. As of 1 October of 2009, the government of Singapore has likewise established Safeguard Singapore to coordinate activities dealing with IT security threats.

Policy Issues – State and Local Coordination

Cybersecurity is in some ways a unique issue because it affects, and is affected by, all levels of global society, from the micro (individuals and small businesses) to the macro (nations and regional infrastructure). Therefore, it is widely recognized that engagement with local authorities and even individuals is a key aspect of securing cyberspace. These issues can be technological, such as fostering development of better security products for personal computers and for information assurance. It can also be educational, such as providing information to the public on the nature of cyber threats and cyber crime, the importance of regularly changing passwords, or best practices for security protocols for small businesses.

It can also involve assistance to state and local governments in developing policies to secure their networks, or in developing appropriate laws and regulations for systems affected by

cyberspace, or for prosecuting cyber criminals. While some countries have developed mechanisms to deal with these more local issues, large areas of the globe are still the cyber "wild west". Because of the strong interconnectivity of global cyber networks, these unregulated regions can be havens for many kinds of malicious actors who increasingly can operate globally from almost any point of origin. Within the USG, DHS has instituted a variety of outreach programs to coordinate and provide resources to State and local authorities. A recent study by Center for Strategic and International Studies has even proposed the organization of a National Town Hall on cybersecurity issues.

Policy Issues – Private Sector Organization

The private sector is an extremely important element of the cybersecurity landscape. One reason is that a large fraction of cyber assets and critical infrastructure lie within or are fully owned and controlled by private groups. Moreover, the private sector is increasingly the target of a wide array of malicious cyber activity. These include theft of intellectual property, commercial espionage, database corruption, denial of services, identity theft, and even cyber extortion. The financial services industry is a prime target of such activities, and even single cyber events have cost industries tens of billions of dollars in losses. The telecommunications industry is an increasingly attractive target with hackers attempting to co-opt and program millions of cell phones simultaneously for ill use. Because of increasing use of computer and communications technologies for sensing and control, the transportation industry has become increasingly vulnerable to cyber threats, and is one of the prime targets of potential military or terrorist attacks. The energy and utility sectors have significant vulnerabilities which are increasingly severe because of the possibility of major disruptions to electric power, water, and oil and gas flows. It is estimated that global utility operations are attacked by hackers or malicious code up to 1000 times each year.

The private sector within the US has been proactive in organizing and coordinating resources for prevention, response, and recovery to cyber events, and for funding of R&D. These include informal collaborations within industries and sharing of best practices. It also includes a variety of public-private organizations between USG, state, and local authorities, as well as industry partners, academics, think tanks, and interest groups. These include he Business Software Alliance, the Cybercrime Institute, the Electronic Crimes Task Force, the National Cybersecurity Alliance, and the Anti-Phishing Working Group. Because of the size of the sectors involved, these groups have potentially large resources to bring to bear and significant reach. They are also a template for what could be done internationally in organizing private sector resources where public regulation or resources are insufficient.

Policy Issues – International Coordination

Because cyberspace is increasingly becoming a common global priority, many believe a much more serious view of its international implications and regulation must be taken. Such efforts could be directed to sharing of security technologies, development of international security standards, information sharing and coordination between national law enforcement agencies, sharing of best practices, and crafting of treaties on its use and misuse. These efforts, however, are still largely in their infancy, likely due to the novelty of the technology, policy, and regulatory landscape.

One increasingly important international cyber issue lies at the defining boundaries between a cyber nuisance, a cyber crime, cyber terrorism, and an act of war. For example, currently there is still no international agreement on how the Law of Armed Conflict (LOAC) applies to cyber operations. The LOAC has traditionally been applied to physical confrontation on land, sea, air, or space, but its extension to cyberspace remains vague. Even the application of the UN Charter to cyber operations is unclear since the "unlawful use of force" provision has historically

been interpreted only in terms of physical violations. Cyber operations present many "gray areas" including the case of a cyber attack originating from outside a country (but of unclear origin) which causes significant damage to a nation's infrastructure, and potentially loss of life. Resolving such questions of international law is of extreme importance because they govern definitions of "acts of war", and how a nation defines its proportional response to them. As cyber terrorist events, and even state sponsored cyber operations against other nations, continue to increase, lack of clarity in international law is becoming an increasingly serious issue.

International activities coordinating cooperation on cybersecurity have unfortunately been somewhat few. One exception has been the issuance of the March 30, 2009 EU Memo IP/09/494, which outlines a cybersecurity strategy for its member states and private sector partners. Additionally, in late 2007 NATO established a Center of Excellence on Cooperative Cyber Defense, which funds cybersecurity policy research and has held a major international conference on the international legal frameworks for cyber conflict.

Many of these challenges have technological factors at their core. The attribution problem discussed previously and the ability to analyze massive amounts of threat-related information and disseminate it in a secure and effective fashion are examples of current importance. Such an international dimension to these issues would seemingly motivate more serious efforts at international cooperation in R&D to address common technology challenges. However, outside of the defense communities, there is currently relatively little international cooperation on cyber R&D. The one notable exception is the research funded by Science and Technology Directorate of the OECD. A more coordinated international response would seem not only to make sense, but perhaps will be critical as cybersecurity increasingly becomes a truly global problem.

Conclusion

This **ISGP White Paper** attempts to assess and characterize some of the significant S&T options and policy issues that surround ***Cybersecurity***. The urgent need to identify "actionable decisions" that lead to practical policies is apparent. The realities are potentially dire, the challenges significant, and while the S&T opportunities are encouraging, almost all require further maturation and an expansion of our physical and societal infrastructure.

Overall, potential solutions contain elements of near-, mid-, and long-term planning based on integrated domestic and global policies. The most attractive near-term options capitalize on currently accessible S&T approaches that require support by consensus. Mid-term options need to harness evolutionary progress, largely involving S&T research and development often already underway. In the foreseeable future, these mid-term options are likely to have the largest impact on optimizing the world's ability to meet its domestic and global energy needs. Long-term options can be realized only from investments in R&D that challenge the existing S&T understanding and fundamentally change the technological opportunities available to transform our access to sufficient, environmentally safe energy resources. Policy decisions need to consider how to integrate all three types of options into a globally supported direction since no single S&T approach can be expected to be sufficient to meet the scale of the recognized challenges associated with ***Cybersecurity***.

A comprehensive **ISGP Program on *Cybersecurity*** would examine the topic in detail, develop a **Strategic Roadmap on Cybersecurity** from extensive interviews and a through review of the literature, and utilize the ISGP's unique format of critical debates and caucuses extending over a two-three year series of interviews and international conferences to help shape domestic and international policies.

