JPCERT CC®
Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

The Cyber Green Initiative:

Improving Health Through Measurement and Mitigation

A JPCERT/CC Concept Paper
August 10, 2014

Concept Paper: Table of Contents

Executive Summary

This paper provides the conceptual basis of the Cyber Green Initiative (CGI), and includes a description of its rationale, key definitions, existing efforts, and its proposed mission. CGI's core focus is on tapping the collaborative potential of stakeholders in cyberspace through promoting the concept of "cyber health" and establishing a reliable platform for generating cross-comparable statistics. CGI will focus on the following core tasks: establishing reliable cross-comparable statistics and information sharing mechanisms, enabling operational remediation efforts, and providing insight into systemic risk conditions in the cyber ecosystem. After an initial discussion about CGI's background, the concept paper includes the following:

Building on Past and Existing Efforts (p. 7): The Concept Paper describes past and existing efforts in public health and cyber security, as well as lessons that will inform the resulting CGI and its operations. The paper examines the following:

- Leveraging the Public Health Model, Applied to Cybersecurity;
- CERTs/CSIRTs Collaboration;
- Past Botnet Reduction Efforts;

- Metrics/Measurement Efforts;
- The Importance of a Common Taxonomy;
- Benefits for Cyber Security Stakeholders.

Establishing the Cyber Green Initiative (p. 13): The paper describes the two-phase process in which CGI will develop:

- Phase 1: Identifying data sources, developing cross-comparable metrics, and establishing a reliable portal for information sharing.
- Phase 2: Expansion of the CGI mission, and maturing CGI capabilities.

Appendix A, Cyber Green Public Health Workshop (p. 16): Appendix A provides an anonymized transcript of a Public Health Workshop, conducted on June 4, 2014 at the Delta Risk office in Arlington, Virginia. Workshop discussion addressed examples of practices, metrics, and information sharing approaches used by public health organizations including the World Health Organization (WHO), the Centers for Disease Control (CDC); and the Department of Homeland Security (DHS) National Biosurveillance Integration Center (NBIC).

Introduction to the Cyber Green Initiative (CGI): Defining Cyber Health

The driving concept behind CGI comes from approaching global cybersecurity from a health perspective, rather than a national security perspective. It focuses on the identification of underlying factors in the global cyber ecosystem that poses a risk to stakeholders across the globe, then enabling remediation for those who can act. CGI is intended to be collaborative rather than divisive, and proactive rather than reactive.

Thus, it is imperative that we first define the concept of "Cyber Health" as a basis for discussion about CGI's mission and organization. "Cyber Health" is defined as, "a condition of cyber systems and networks that are not only free from infection from malware and botnets but also contributes more broadly to the overall trust and usability of the cyberspace for the well-being of all.[1]" This definition helps to clarify what a healthy cyber ecosystem is, and will provide future CGI stakeholders a consistent definition that will enable effective participation.

Background

The international community has grappled with the challenge of achieving meaningful cooperation in cyberspace for some time. Particularly in recent years, cyberspace has been increasingly characterized as a competitive environment more prone to conflict rather than cooperation, moving away from the original concept that cyberspace is a shared global resource that fosters an open environment for all to interact and share information. Distrust in cyberspace increased with more nation states acquiring and employing offensive cyber capabilities, leading some to advocate a need for greater national control of cyberspace akin

[1] Yurie Ito, "Managing Global Cyber Health and Security through Risk Reduction." July 18, 2011.

to raising walled fences. This growing atmosphere of distrust in cyberspace raised concerns about a "balkanization" of the Internet, contrary to the core values upon which various stakeholders have built and managed this shared resource.

However, such hyperbolic characterization of cyberspace as a primarily competitive environment can be misleading. In fact, many actors facing complex international issues find that cooperation is also just as necessary, and there is also potential for cooperative structures to emerge in cyberspace.[2] Actors will find themselves in cyber conflict in some cases, but simultaneously find that for many other issues—such as botnet reduction—cooperation is both needed and mutually desirable in order to enhance each other's overall security in cyberspace. Furthermore, the transnational nature of cyber risk and the involvement of both state and non-state actors increase the importance of achieving cooperation in a way that brings together previously discordant communities. When such cooperation can occur, the collective benefit that emerges for all participating actors may be greater than the mere sum of their individual actions.

The challenge lies in that despite recognizing the benefits of cooperation in principle, individual actors often fail to achieve cooperation naturally under a state of "anarchy."[3] As Jean-Jacques Rousseau's story of the Stag Hunt illustrates, individuals may still choose to hunt a small hare for themselves rather than participate in a group hunt for a large deer despite a better payoff, depending on conditions of the environment such as risk.[4] Both independent action (hare hunting) and collaborative action (stag hunting) are rational choices for each actor to make, depending on their expected weight of personal risk versus mutual benefit. When faced with these two choices, factors such as trust among players and environmental structure play a significant role in creating an environment more conducive to cooperation.

In cyberspace, such conditions that foster cooperation are still in their nascent stages. Despite the existence of common underlying challenges that undermine the health of the overall ecosystem, and the existence of efforts to mitigate such problems by individual entities, sustained and robust cooperation in this domain has yet to occur. The lack of reliable global regimes for coordination, uncertainties about the benefits of cooperation, concerns about the sharing of sensitive information, and the lack of appropriate global norms have kept stakeholders from reaching potential collaboration.

The Cyber Green Initiative (CGI) aims to facilitate such cooperation and trust among key stakeholders for the continued robust utilization of cyberspace for routine communications and activity. In this regard, CGI promotes approaching global cybersecurity from a public health perspective, aimed at improving the "health" of the global cyber ecosystem. CGI's

[2] Thomas Schelling, "An Essay on Bargaining."
[3] Axelrod and Keohane, "Achieving Cooperation Under Anarchy."
[4] Rousseau, *A Discourse on Inequality*, "If it was a matter of hunting a deer, everyone well realized that he must remain faithful to his post; but if a hare happened to pass within reach of one of them, we cannot doubt that he would have gone off in pursuit of it without scruple." and Brian Skyrms, *The Stag Hunt and the Evolution of Social Structure*

primary mission will be to motivate stakeholders at the international, national, and local levels to participate in coordinated remediation and prevention activities, by establishing robust metrics and standards for cross-comparable cyber risk measurement as well as mechanisms for sharing actionable information for timely, coordinated measures.[5]

Cyber Health: Applying Lessons from Global Public Health

Traditional approaches to cybersecurity from a national security or law enforcement perspective have their limitations in that they mainly take reactive postures to threats or incidents. They also rely heavily on the decision making of nation states rather than a variety of key stakeholders comprising the cyber ecosystem. Such approaches often overlook proactive measures to improve underlying conditions and do not necessarily reduce risk at a systemic level. Such approaches are analogous to treating a case of malaria through medicine, while leaving the nearby mosquito swamp untouched or developing cancer treatment technology while paying little attention to the population's tobacco use.

With these reasons in mind, CGI aims to promote the concept of cyber "health."[6] The advantages of approaching global cybersecurity issues from a public health perspective are that it compels stakeholders to act based on an inclusive, holistic view of security. The focus is not only on response to threats and incidents, but also on proactive measures to improve a system or network's general resiliency. As stakeholders increasingly approach global cybersecurity from a public health perspective, they will not only mitigate malicious activity on their respective networks and systems, but will also view their activity as one part of a larger effort to make the global cyber ecosystem clean, safe, and reliable.

Much can be learned from the missions of global health organizations such as the World Health Organization (WHO) and national-level agencies such as the U.S. Centers for Disease Control and Prevention (CDC). Their missions include limiting the spread of infectious diseases, information sharing and response to outbreaks, as well as prevention measures such as immunization, education and awareness campaigns about hygiene, and the development of key metrics and standards in medicine. These organizations, by pooling resources at the local, state, national, and international level in a coordinated fashion, have been playing a central role in combating complex transnational challenges and have been tremendously successful in improving global health conditions.

Likewise, the establishment of initiatives in cyberspace focused on prevention and remediation at a global scale has potential to bring together previously disjointed efforts to secure the cyber ecosystem and develop common norms on cyber health. Currently, many cyber risks faced by public and private sector entities are symptoms enabled by an "unhealthy" cyber ecosystem, such as the prevalence of botnets and the unabated spread of malware. A collaborative and concerted effort to target such underlying causes of systemic

[5] A discussion on the importance of cross-comparability of statistics is available on pg.5.
[6] Yurie Ito, "Managing Global Cyber Health and Security through Risk Reduction." July 18, 2011.

cyber risk, rather than merely mitigating its symptoms, will have far-reaching impacts in establishing confidence in the safety and resiliency of the global cyber ecosystem.

Cross-Comparable Statistics Are Key

One of the most important conditions for enabling robust cooperation in cyberspace is the availability of cross-comparable statistics that empower decision makers to set policies based on evidence, establish priorities, and see trends. The key focus is on making various statistics produced at the national and organizational level *cross-comparable,* rather than the merely sharing information. Today, many national-level CERTs and CSIRTs around the world generate their own statistics from internally collected data. The problem is that data collection varies greatly, dependent on CERT/CSIRT capabilities and mandates. These data are then turned into statistics using a range of different standards and methods. Added to that are third-party data providers that also use their own data collection and statistical methods.[7] This becomes a significant impediment to collaboration as decision makers end up comparing apples to oranges and cannot generate meaningful aggregate statistics for use.

There are generally two approaches to achieving cross-comparability: establishing standards *pre-collection* and encouraging each entity to adhere to them when producing statistics, and developing statistical methods *post-collection* to adjust for differences and normalize statistics to maximize comparability. The two approaches are not mutually exclusive, and organizations have relied on both to produce meaningful information for stakeholders.

For example, WHO, for producing global statistics on health risk factors such as obesity and blood pressure, maintains the WHO Indicator and Measurement Registry (IMR). IMR is a central source of metadata of health-related indicators that include indicator definitions and codelists, data sources, methods of estimation.[8] It further provides a mechanism for interoperability through the SDMX-HD indicator exchange format, allowing entities to incorporate appropriate international standards such as SDMX Metadata Common Vocabulary (MCV), ISO 11179, Data Documentation Initiative (DDI), and Dublin Core (DCMES). IMR provides an avenue for individual organizations to achieve harmonization without imposing mandatory standards. Additionally, WHO also uses statistical methods to make adjustments to national-level data, adjusting for factors such as risk factor definition, age groups for reporting, reporting year, and representativeness of population. WHO also takes into account uncertainty in estimates and produces age-standardized comparable estimates, and publishes its statistical methods online for transparency.

Several principles are imperative in achieving cross-comparability using the above two approaches. First is a focus on enabling voluntary adoption of good standards rather than issuing mandates. Individual organizations often have vastly varying capacities and operate in different environments, and imposing high standards may hinder data collection and

[7] "CSIRT Statistical Indicators Working Paper." OECD Working Party on Information Security and Privacy (WPISP).
[8] "Indicator Registry," World Health Organization, http://www.who.int/gho/indicator_registry/en/

reporting itself. Instead, developing frameworks such as IMR make available user-friendly databases for access, comparison, and translation of data that better meets international standards. Second is an emphasis on transparency. When possible, information such as data sources, sampling methods, and methods for estimation should be made available in a transparent and accessible manner. The disclosure of such information builds confidence and trust in the system, and encourages open discussion about improving methodology and analysis techniques.

The potential for global collaboration stemming from cross-comparable statistics in cyber health is enormous. Decision makers across the world in various industries will be able to not only see which regions have the greatest botnet infection rates and which regions have the most unpatched systems, but over time also see trends such as activity patterns, or the "half-life" of zero-day vulnerabilities. Such statistics would enable individuals to make decisions based on evidence rather than perception, and help justify investment and budgetary decisions as well as help make predictions based on patterns. Most importantly, these statistics enable organizations such as CERTs to mitigate underlying risk factors and provide a way to measure their progress.

Building on Past and Existing Efforts

A. Leveraging the Public Health Model in Cybersecurity

The application of public health models in cybersecurity is not a new concept. As early as 1996, a DARPA-sponsored RAND report recommended that one of the steps that USG could initiate immediately to reduce U.S. vulnerability in cyberspace was to adopt the information sharing functions of the CDC.[9]

> "The CDC acts as a worldwide clearinghouse for health and disease information; it is a central source of information when needed, from routine queries to tracking the spread of epidemics. This same clearinghouse function is needed to collect and assess information on disparate cybersecurity incidents."

The RAND report, however, mentioned this possibility only briefly and did not extend the application beyond information sharing. The analogy between public health and cybersecurity grew stronger as the number of Internet users skyrocketed and more networks and systems came to be interconnected, resulting in a global "cyber commons."[10] Computer security expert and biostatistician Dan Geer says that like in dealing with cybersecurity challenges, public health practitioners focus on "macro scale effects due to

[9] "The Day After… in Cyberspace II: An Exploration of Cyberspace security R&D Investment Strategies for DARPA" RAND, 1996

[10] Author acknowledges that this characterization is not wholly accurate, as such networks and systems are bound to physical infrastructures often within a state's jurisdiction and thus is not a globally shared resource. The characterization nonetheless is used to explain the wide reach and interconnectivity of cyberspace.

micro scale events."[11] Due to the high degree of interconnectivity and rapid transmission of information in cyberspace, approaches to public health came to be viewed as increasingly applicable. From 2010 to 2012, various reports exploring this nexus have been published, each from a distinct perspective.

In 2010, Rattray, Evans, and Healey extensively explored this model in a Center for a New American Security (CNAS) report, exploring how concepts such as epidemiology and preventive health can be applied in cybersecurity.[12] The chapter focused on measures used by epidemiologists to prevent and respond to disease outbreaks, including sanitization, diagnosis, early warning, and isolation. The report conducted a comparison of outbreak alert systems to existing cyber incident alert systems, as well as a comparative analysis of WHO and CDC. Finally, the authors recommended that U.S. should lead global efforts to clean up the cyber environment, while realizing the limits of achieving security through deterrence in cyberspace.

Scott Charney, leader of the Trustworthy Computing Group at Microsoft, took a slightly different approach by framing the topic under collective defense.[13] While focusing on the idea of "device health" and the proposition of issuing health certificates to consumer machines before allowing Internet access, much of the analogy remained in achieving international cooperation in collectively defending against a threat, which does not address the public health focus on proactive measures. Collective defense is contingent on a premise of shared threat; in cyberspace, however, not every actor shares the same threat perception, nor do some of the underlying risk factors constitute threats in and of themselves. Just as WHO not only responds to pandemics such as SARS but also researches tobacco use and obesity, CGI's mission must look beyond the collective defense analogy.

In 2011, the Department of Homeland Security (DHS) published "Enabling Distributed Security in Cyberspace," which focused on building a healthier cyber ecosystem by increasing automation.[14] DHS proposed that in the face of increasing cyber attacks that propagate at machine speeds, we must explore ways to have cyber devices to "work together in near-real time to anticipate and prevent cyber attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state." This model draws upon the immune system of the human body rather than a public health model, and cites interoperability and authentication as also important for building a healthier cyber ecosystem. The report mentions that incentivizing individuals to adopt cyber best practices and configuration guidelines remains a challenge, stemming from the difficulty in defining a level of harm incurred as a result of a cyber incident. The report recommended that a "Cyber CDC" in the future should provide stakeholders with the

[11] Dan Geer, "Measuring Security"
[12] Rattray, Evans, and Healey, "Chapter 5: American Security in the Cyber Commons," *Contested Commons: The Future of American Power in a Multipolar World.* P.139-176
[13] "Collective Defense: Applying Public Health Models to the Internet" Scott Charney, Microsoft, 2010
[14] "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action" DHS, March 2011

information needed to diagnose problems through increased sharing of anonymized cyber incident and mitigation data.

Finally, the East West Institute (EWI) published "The Internet Health Model for Cybersecurity" in 2012, presenting a comprehensive overview of functions in public health that could be applied to cybersecurity. Like others, EWI also looked to WHO and CDC, and identified five basic functions as applicable: education, monitoring, epidemiology, immunization, and incident response. It also outlines some limitations and dangers of relying on the public health analogy, such as how malware originates with human intent but that diseases are organic, that devices do not have natural immune systems, and the negative connotations associated with surveillance and quarantine in cyberspace. Most importantly, the EWI report notes that while individuals must take ultimate responsibility for their online safety, they cannot do so in isolation. In this regard, EWI notes the importance of establishing sound metrics, measurement, and information sharing schemes to provide the foundations of cooperation.

To move toward a cybersecurity approach that implements lessons from the public health model, CGI seeks to enable similar collaborative information sharing processes between CERTs and CSIRTs. Based on the work of global public health organizations, CGI will identify comparable risk conditions in cyberspace, and empower stakeholders to remedy those fundamental issues.

B. CERTs/CSIRTs Collaboration

National level CERTs and CSIRTs have collaborated with each other in varying degrees over the years. The most salient example would be the Asia Pacific Computer Emergency Team (APCERT) established in 2003 to facilitate timely international cooperation in incident response among members and enable information sharing and technology exchange. APCERT currently has 25 member teams from 19 economies. APCERT operates five working groups focusing on issues such as information sharing and establishing a common platform for threat monitoring, and holds regular joint exercises on simulated incidents.

APCERT, however, is not without its challenges. According to APCERT's 2013 Annual Report, APCERT's key mission in the future is to develop ways to measure the prevalence of malware and the success of remediation. However, it mentions that one of the challenges is a lack of cross-comparable data sources that are robust enough to measure national and global level risk. The lack of common metrics serves as a barrier to establishing a common language between the policy and technical arena (see Section D, "Metrics/Measurement Efforts" and Section E, "Importance of a Common Taxonomy" for further discussion on these issues).[15]

Similar efforts include organizations such as TF-CSIRT in Europe, which promotes collaboration among European CERTs and neighboring regions as well as maintaining liaison relationships with organizations such as FIRST and ENISA. However, its functions are more

[15]"APCERT Annual Report, 2013," APCERT, http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2013(FINAL).pdf

limited than APCERT to a forum for the exchange of experiences and knowledge. Similarly, the Forum of Incident Response and Security Teams (FIRST) is a global forum of national level CERTs, but the organization does not facilitate cooperation at an operational level. Still, many national-level CERTs continue to collaborate in ad-hoc fashion on a case-by-case basis and provide a foundation for CGI efforts.

At this point, many CERTs recognize a need to mature their respective capacity and have focused on certain efforts to improve interoperability and measure performance. One of the areas that FIRST has focused on in the past is the development of the Common Vulnerability Scoring System (CVSS) that sought to provide a universally open and standardized method for rating IT vulnerabilities. CVSS has since been incorporated into the ITU-T Cybersecurity Information Exchange Techniques (CYBEX) framework, which establishes standards for structured information exchange at known assurance levels. FIRST is also conducting research into vulnerability data exchange mechanisms through the Vulnerability Reporting and Data eXchange Special Interest Group (VRDX-SIG).

In light of lessons from these past efforts, CGI will establish itself as a hub for collaborative information sharing. To do so, CGI will focus closely on ways to improve interoperability for all participants. As CGI matures, it will expand on this role by providing capacity building support for participants as well.

C. Past Botnet Reduction Efforts

One of the biggest underlying risk conditions that contribute to an unhealthy cyber ecosystem is the prevalence of botnets in a given region. In the past, there have been several national-level efforts to mitigate botnets within their jurisdiction, such as those of Finland, Australia, Japan, Korea, and Germany. Among the most notable efforts is the Australian Internet Security Initiative (AISI) established in 2005 and operated by the Australian Communications and Media Authority (ACMA), which collaborates with 139 ISPs. AISI collects data from various data sources that exhibit botnet behavior, then provides reports to ISPs of compromised IP addresses, at which point the ISPs can then notify their customers about the infection. In addition, the AISI launched the iCode, a voluntary ISP code of practice that aims to promote a security culture in the industry. AISI is currently planning to develop an online portal accessible to Australian ISPs, which will make available current and historical malware compromise data relating to each ISP's respective network, as well as more comprehensive data about a particular malware compromise. The portal is expected to be operational in 2014.[16]

Other national-level botnet cleanup efforts share similar operational models. For example, the Anti-Botnet Advisory Centre operated by the Association of the German Internet Industry cooperates with 11 German ISPs and two Anti-Virus vendors and makes available the EU-cleaner, free software that users can download to clean up their computers. Though

[16] "Australian Internet Security Initiative," ACMA.au.gov, http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative#aisi_iia

discontinued, Japan's Cyber Clean Center (CCC) operated from 2006 to 2011 through collaboration between Telecom-ISAC Japan, JPCERT/CC, Information-Technology Promotion Agency, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade, and Industry. CCC cooperated with 76 ISPs and 7 Anti-Virus vendors.

Other than national level efforts, corporations such as Microsoft have been participating in botnet reduction activities as well. Microsoft's Digital Crimes Unit (DCU) collaborates with multiple international and national law enforcement agencies to take down botnets enabling cyber crime. For example, in December 2013, Microsoft collaborated with Europol and FBI to disrupt the Sirefef/ZeroAccess botnet which infected nearly two million computers. Although they were not able to completely eradicate the botnet, which is remotely controlled from thousands of different computers, they were able to significantly disrupt its effectiveness.[17] In June 2013, Microsoft also successfully collaborated with FBI to take down more than 1,400 Citadel botnets, cleaning up more than 2 million computers worldwide. Microsoft is working to launch the Cyber Threat Intelligence Program (C-TIP), which makes information about botnet inflections available online.

The major difference between national botnet reduction models and Microsoft's model is that national models focus on enabling individuals to clean up their own computer systems from being part of a botnet, while Microsoft will actively target the command and control servers of botnets through collaboration with law enforcement agencies. Both approaches have their merits for overall botnet remediation, and it would be CGI's role to generate robust aggregate statistics and analysis to enable such stakeholders to conduct remediation activities more effectively and collaborate more easily when necessary.

D. Metrics/Measurement Efforts

Many cybersecurity experts and organizations have come to the realization that creating robust metrics and measurement practices not only reduces uncertainty and fear around security measures but also enables better decision-making based on evidence. Computer security expert Dan Geer, in his tutorial "Measuring Security," has explained the significance of establishing good metrics and measuring as a first step in security risk management, and provided examples of how statistics have been applied in sectors such as public health, insurance, and portfolio management.[18] Since then, conferences such as Metricon that occurs concurrently with the RSA conference have focused specifically on establishing robust cybersecurity metrics. For example, during 2014's Metricon 9, Christophe Huygens presented "Methods for Large Scale Measurement of the Security of Internet Ecosystems,"

[17] "Microsoft, Europol, FBI, and Industry Partners Disrupt Notorious Zero Access Botnet that Hijacks Search Results," Blogs.Technet.com, http://blogs.technet.com/b/microsoft_blog/archive/2013/12/05/microsoft-europol-fbi-and-industry-partners-disrupt-notorious-zeroaccess-botnet-that-hijacks-search-results.aspx

[18] "Measuring Security," Dan Geer, http://geer.tinho.net/measuringsecurity.tutorial.pdf.

which explored the use of empirical experiments for large-scale analysis of mixed web content, etc.[19]

At FIRST, the Metrics SIG is currently working to improve CSIRT processes and metrics as a means to improve incident response and management. Similarly, OECD's Working Party on Information Security and Privacy (WPISP) began a project on improving the international comparability of statistics produced by computer security incident response teams. In its initial working paper, OECD WPISP identified several CSIRT statistical indicator categories and is currently working to establish robust metrics for each category.

CGI will build on the lessons from these efforts, and incorporate metrics that are gathered globally. Regardless of whether data is gathered, metrics will allow for effective comparison of data. Metrics will also allow CGI to understand cyber environmental factors that enable cybersecurity problems and threats. CGI will also be able to measure the performance of its metrics over time by assessing whether they help to decrease botnets, certain types of attacks, or other problems. These practices will reinforce strong global participation by CERTs/CSIRTs, and will help to achieve an accurate picture of global and regional cyber health.

E. Importance of a Common Taxonomy

For CGI, sound metrics and measurement practices are only one part of an effort to ensure that members of the international CERT/CSIRT community can collaborate to improve global cyber health. Stakeholders require a common taxonomy so they may develop a consistent understanding of the analyses and metrics provided by CGI.

The Structured Threat Information eXpression (STIX), developed by Mitre, is a standardized language for cyber threat information sharing. The Trusted Automated eXchange of Indicator Information (TAXII), also developed by Mitre, serves as the messaging exchange service that transmits threat information in STIX language. Government and non-governmental organizations are increasingly relying upon STIX and TAXII for information sharing purposes, as they help to simplify communication. CGI use of features such as STIX and TAXII will help enable the use of a common language, and will further empower CERTs/CSIRTs in their remediation efforts.

F. Benefits for Global Cyber Security Stakeholders

In its efforts to produce a healthier global cyber ecosystem, it is clear that CGI success will serve the public good at an international level. Encouraging collaborative behavior, deemphasizing political and national security conflict, promoting cyber health metrics, and enabling Internet functionality and reliability will benefit the global cyber commons.

[19] "METRICON 9, Full Proceedings." https://dl.dropboxusercontent.com/u/43553/METRICON-9-Full-Proceedings.pdf

However, CGI will also provide more concrete benefits to a variety of specific cyber security stakeholders throughout the world:

CERTs/CSIRTs: For CERTs/CSIRTs, CGI will enable their remediation efforts and foster new levels of collaborative information sharing. CGI will allow the global CERT/CSIRT community to gain new insights through its implementation of sound health metrics and common taxonomy. Cyber Green will allow these organizations to clearly assess their own progress against other parts of the globe to an extent not yet achieved by other collaboration programs.

Data Providers: CGI's incorporation of critical data sources will allow data providers throughout the world to evaluate gaps in their current products. By serving as a hub for cyber collaboration, data providers will have a centralized source for assessing the effectiveness of data sets they maintain. Assessing strengths and weaknesses will allow these organizations to fine-tune their products for consumers, researchers, and other interested cyber security stakeholders.

Benefits to Other Key Stakeholders: As CGI matures and is able to expand its mission, other global cyber security stakeholders will to realize substantial benefits as well. Governments, multinational companies, and non-governmental organizations may also be able to gain insights into sound cyber security practices and behaviors, based on CGI successes achieved during Phase I.

Establishing the Cyber Green Initiative

CGI, acknowledging past and current efforts to improve cyber health, seeks to establish itself as an increasingly effective hub for collaborative efforts to address systemic cyber risk and improve the general health of the cyber ecosystem. The initiative seeks to unlock the vast cooperative potential in this area that has yet to be realized. CGI's core approach is to improve cyber health through measurement and mitigation, and will focus on the following core tasks:

- Establishing Reliable Cross-Comparable Metrics and Information Sharing Mechanism
- Enabling Operational Remediation Efforts
- Providing Transparency into Risk Conditions of Cyber Ecosystem across the Globe

CGI must clearly identify the key stakeholders to be involved in this process. It must operate according to an inclusive, multi-stakeholder approach. Currently, CGI seeks to work closely with the following:

- The CERT/CSIRT community
- Organizations, both commercial and non-profit, that are sources of data related to cyber health and risk

- Research organizations and individuals specifically focusing on measurement of cyber health and risk factors
- Experts knowledgeable in organizational models, data gathering, analysis and measurement related to public health

CGI is currently planned to launch in early 2015 with initial support from JPCERT/CC and the Japan Ministry of Economy, Trade, and Industry (METI). CGI plans to build its capacity in two distinct phases. Phase 1 will focus on establishing a sound platform for injecting appropriate data sources, aggregating and analyzing them to generate meaningful statistics, and disseminating them to key stakeholders. Phase 2 will seek to build on the CGI platform by expanding CGI missions into areas such as capacity building for national-level CERTs on metrics and measurement, using the repository of statistics to generate deeper analysis on salient cybersecurity issues, and expanding and diversifying its user base.

A. Phase 1: Cross-Comparable Metrics and Information Sharing Mechanism

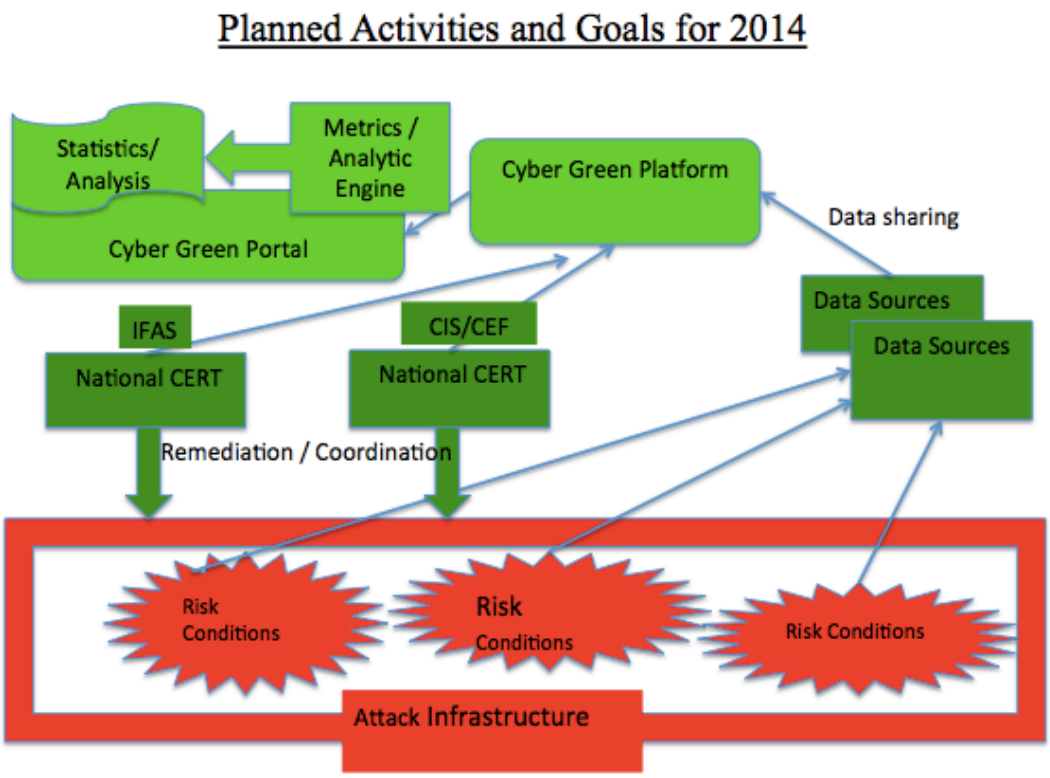

Figure 1. CGI Planned Activities and Goals for 2014

Phase 1 of CGI involves building a foundation for the following three areas:

- Identification of critical data sources and establishment of mechanisms to inject data into the CGI platform

- Development of cross-comparable metrics and indicators to aggregate and analyze injected data
- Establishment of a reliable portal for the easy access and dissemination of generated statistics and information

For Phase 1 of CGI to be effective, it would be important to first carefully select and define major risk conditions that contribute to an unhealthy cyber ecosystem. Next data sources that allow for the measurement of these risk conditions will need to be identified and arranged for injection into the CGI platform. These data sources, when possible, will come from publically available sources allowing for easy data sharing arrangements. Once data sources have been aggregated and adjusted through the CGI platform, national-level CERTs will be able to access the platform to obtain actionable information for remediation and collaboration. The aggregated data available on the CGI platform will then be further analyzed to generate various statistics for use by a wider range of CGI stakeholders such as research organizations.

B. Phase 2: Expansion of Mission

Beyond the initial standup of CGI following the model according to Figure 1, the organization will seek ways to mature its operations in Phase 2 by maintaining three focus areas:

- Focus on Deeper Analysis: CGI can use the repository of data and statistics to generate deeper analysis on salient cybersecurity issues, which could be expanded into functions such as malware "epidemiology" that provides necessary information for faster and more effective remediation. Over time, the consistent measurement of risk conditions will also enable the generation of trends.

- Focus on Enabling Participants: In order to facilitate the effective utilization of CGI statistics, the organization can develop programs for CERT capacity building dedicated to metrics and measurements. CGI can also serve as a repository for best practices on standards development and information sharing mechanisms. CGI can hold workshops with a wider community of stakeholders for the purpose of discussing expanded applications of CGI-generated statistics for research and innovation. Such efforts will not only expand and diversify its user base, but also enable each stakeholder to utilize CGI statistics to its full extent.

- Focus on Norm Development: One of CGI's key objectives are to foster a healthier cyber ecosystem by increased cooperation and joint remediation efforts. Not only will CGI participate in technical measurement and remediation efforts, but also raise awareness and promote the concept of "cyber health" to a broader audience. Part of these efforts may include outreach activities to encourage more ISP participation as well as encouraging corporations to contribute to cyber health.

In addition to the above Phase 2 measures, CGI may examine ways to increase and diversity its member base. With a broader base of participants, CGI's cyber health emphasis and approach will be strengthened by broader "buy-in" from the CERT/CSIRT community. Other stakeholders in government and civil society may also take note of the analytic products, capacity building, and norms supported by CGI. In this way, Phase 2 will further strengthen international support for an overall cyber health approach to cybersecurity.

Making Cyberspace Healthier Through the Cyber Green Initiative

As CGI approaches its first phase of implementation, present-day cyber conflict, the growth of botnets, and the prevalence of malware all serve as signs that a global collaborative approach to cybersecurity is needed now more than ever. Applying the lessons of global health approaches, defining cyber health, and converting threat information into practical metrics will help CGI and its future CERT/CSIRT partners improve the cyber ecosystem. JPCERT/CC looks forward to developing, implementing, and refining this model in conjunction with members of the global CERT/CSIRT community. Through collaboration between the members of this community, CGI will improve cyber health for all global users.

APPENDIX A: CGI Workshop on Applying Public Health Models to Cyber Security

Workshop Overview: On June 4, 2014, JPCERT/CC convened a workshop on the application of public health models to cyber security. CGI, by approaching global cyber security from a public health perspective, looks to make the global cyber ecosystem healthier by coordinating between private and public stakeholders at the international, national, and local levels. To this end, CGI will establish robust metrics and standards for cross-comparable cyber risk measurement, and will disseminate actionable information for timely, coordinated measures. Going forward, public health topics discussed in the June 4, 2014 workshop will help CGI in identifying the following:

- Valid lessons from past efforts to apply public health models to cyber security;
- Successful organizational models in the public health arena;
- Approaches to information sharing; and
- Ways to develop and improve metrics that measure cyber health.

Based on workshop participant input, the below is a transcript of the Public Health Workshop conducted on June 4, 2014 at the office of Delta Risk. Per the Chatham House Rule, the identities of the participants are not disclosed and their individual remarks in the transcript are not attributed to any individuals who participated in the workshop. Because we use the Chatham House Rule in the transcript below, separate remarks are separated by a single space.

Transcript: Public Health Workshop Proceedings
Below is a transcript of the remarks and proceedings from the June 4 Public Health Workshop for CGI. It is divided into the following sections:

- 1. Introduction of the Cyber Green Initiative
- 2. Current and Past efforts to Apply Public Health Approaches in Cyberspace
- 3. Selected Survey of Organizational Models and Information Sharing Efforts of Public Health Institutions
- 4. Improving Cyber Health: Metrics, Information Sharing, Trust Building, Awareness, and Protecting Privacy
- 5. Limitations of the Public Health Analogy on the Global Cyber Ecosystem

1. Introduction of the Cyber Green Initiative

(*Editor's Note*: The introduction portion of the Workshop included a PowerPoint presentation discussing the concept of the Cyber Green Initiative).

CGI's overarching goal is to establish an effective hub for collaboration efforts which address cyber risk and improve the health of the cyber ecosystem.

The CERT community faces increasing difficulty stemming from national security/nation-state rivalry mentalities in cyberspace. China, Taiwan, Vietnam: all cooperative with JPCERT/CC, for example. This is a significant contrast with national security issues.

[CGI will use] metrics to define cyber health.

In the [first year] for CGI, we'll look at getting good data sources, data likely to be enabling. This will include a Concept of Operations (CONOPS), which will have a First-Year "how-to" for those operating Cyber Green.

Public health emphasizes publicly available data – Cyber Green will have to do more to consider what types of data are economically valuable.

Cyber Green is less focused on cyber "outbreaks" – and is more about "draining the swamp."

There needs to be a discussion about who benefits and who loses under the eventual organizational model.

There may be some value in not spreading information publicly right away. There may be more value in getting information to specific key players first, and JPCERT/CGI may be able to offer this through the portal.

[CGI is] measuring the cyber health of what? An IP block? Region? Subregion?

Generally, the model is based around nation-states.

Mandatory Reporting: What countries have it? Singapore, for some sectors. This is not the case in the US.

2. Current and Past efforts to Apply Public Health Approaches in Cyberspace

Scott Charney's Collective Defense paper – the paper holds good ideas, but the language is still national security-focused.

A paper with DHS and MITRE looked at both public health and biodefense. The latter refers to defense from attack. It also included comparison to evidence-driven medicine. There was an emphasis on practices and technologies – this was more tactical, but still good.

It was focused more on biodefense than on public health. Advantages belong to the attacker. It looks at three things. 1) What were the advantages to the defender? Large, complex systems with connectivity could create a large sensor network, and would aid tactical and policy decisions. Stronger, better data authentication can result. 2) Automation: need this to be able to have good decision-making. 3) Interoperability (with STIX and TAXII as examples of this).

While the above are still related to biodefense, these ideas can enable the public health approach and better data-driven outcomes.

With this in mind, you can start to establish a more valuable set of data. APIs (IFAS, CIS, CEF) can make the data available. The near-term enterprise benefit may be low.

With public health and at CDC, actionable info is in demand. This is less focused on the origin of diseases, etc. [The emphasis was on] three key features: 1) CDC mandatory reporting, 2) the ability to distinguish anomalies from outbreaks, and 3) the use of away teams to address outbreaks.

Scans of random samples – can we ask participants to do this? You could ask participants to roll code as a means of establishing immunity. You can measure this against what was in the field. It's also important to make it harder for "silent failures."

Can there be mandatory reporting of failure?

[For CGI] I think it's more a matter of incentivized reporting.

With the wider dissemination of tools, that allows for a neighborhood watch, making it harder for bad actors to hide.

Consider responses to the Kaminsky DNS bug.

With WHO, consider the SARS example – reporting out of China was slowed due to economic concerns regarding lost revenue from decreased tourism.

With TLP, it would be better to have a means of doing this publicly.

There should be something that is unrefined or public. The refined product should have some sensitivity at first. With what's in the portal, others have some "agency" in the info. You can build delay [of releasing the information] for purposes of maintaining an incentive structure.

3. Presentation on the World Health Organization (WHO), Centers for Disease Control (CDC), and National Biosurveillance Integration Center (NBIC)

This portion of the workshop included a PowerPoint presentation on public health organizations. This presentation examined the relevance of these public health organizations' approaches to cyber security.

[Discussion of overview slide begins]. Like public health, cyber security involves incidents. Cyber incidents are comparable to malaria patient counts. Threat vectors in the public health world can refer to the amount of swamp water and mosquito counts, while they refer to the presence of malware and botnet infection rates in cyberspace. For conditions, the public health world deals with obesity rates, famine, and the prevalence of smokers. In cyberspace, comparable conditions would deal with operating systems updates, education, and readiness.

One difference is that in cyberspace, you are dealing with an adaptive and creative adversary.

[Presenter discusses WHO, and its International Health Regulations, promulgated in 2005. This served as a binding legal treaty for 196 countries, mandating reporting to WHO about events constituting public health emergencies.]

This is similar to the current OECD effort. At some point, their information security work will start to have a normative impact. From there, someday, it may have a regulatory impact.

[Presenter discusses the CDC, and provides an overview of the organization and its initiatives of interest. Presenter compares the Public Health Information Network (PHIN) to the Best Practices Survey on information sharing. PHIN promotes standards and defines functional and technical requirements for information exchanges.]

[In comparison to CDC's mission priorities of promoting healthy and safe behaviors, and its scientific research relevant to public health] These compare to future goals for CGI, which will be spelled out in the CONOPS paper. For year 1, CGI will work toward providing an equivalent of information regarding health threats to communities.

CDC's Health Alert Network (HAN) speaks to another question – how much should be invested in terms of money and effort in stakeholder relations? This could be a limiting factor for CGI.

[Discusses the National Biosurveillance Integration Center (NBIC), its mission priorities, and its Biosurveillance Common Operating Network (BCON).]

At least for year 1, don't focus on parallels to "outbreak" procedures [which BCON may use].

4. Improving Cyber Health: Metrics, Information Sharing, Trust Building, Awareness, and Protecting Privacy

[With CGI] we want to move numbers in the right direction – and make sure they aren't fabricated.

For data providers, there are cross-comparison challenges. We want to incorporate clear numbers. Thus, with the MAPP portal – we'll get it. We will be descriptive more than

proscriptive. We'll try Spam zombies, DNS servers (e.g., those for Heartbleed), botnets, others.

Our goal is to establish a "fingerprint." We need the tools & methodology, as well as measurable information. Linkages – we need to be able to identify spam activities, and determine some causality.

Consider examples like GOZeus, .io, the Palestinian Authorities. Look at Regional Registrars. We can find ways to set out a "filthiness index" for the Internet.

We can help others assess the "filthiness" of the Internet. We'll allow others to develop their index.

This will give them [CERTs/CSIRTs] something they can use.

What authorities do CERTs/CSIRTs have?

JPCERT, for example, does not have "shut-off" authority to quarantine computers from the web. Korean government has antivirus authority.

This could include geolocated IP addresses. With IPv4 and IPv6, APNIC says that yes, IPv6 is a hygiene indicator. CGI could support lesson-sharing, and encourage partners to share their insights on how they'll use data.

For academics, we could convene a group and conduct a metrics workshop.

[CGI should consider] Corporate sponsorship, donations in-kind, leading foundations – this would be good to get for CGI.

CGI will have to look at current funding sources, versus what it may be able to get later on, after year 1.

APPENDIX B: Works Referenced

1. Yurie Ito, "Managing Global Cyber Health and Security through Risk Reduction." July 18, 2011.

2. Thomas C. Schelling, "An Essay on Bargaining," The American Economic Review Vol. 46, No. 3 (1956).

3. Axelrod and Keohane, "Achieving Cooperation Under Anarchy," Cambridge University Press (1985).

4. Rousseau, "A Discourse on Inequality," Constitution.org, accessed August 5, 2014, http://www.constitution.org/jjr/ineq.htm

5. Brian Skyrms, "The Stag Hunt and the Evolution of Social Structure," Cambridge University Press, 2003.

6. “CSIRT Statistical Indicators Working Paper.” OECD Working Party on Information Security and Privacy (WPISP).

7. “Indicator Registry,” World Health Organization, http://www.who.int/gho/indicator_registry/en/

8. “The Day After… in Cyberspace II: An Exploration of Cyberspace security R&D Investment Strategies for DARPA” RAND, 1996.

9. Dan Geer, “Measuring Security.” http://geer.tinho.net/measuringsecurity.tutorial.pdf

10. Rattray, Evans, and Healey, “Chapter 5: American Security in the Cyber Commons,” Contested Commons: The Future of American Power in a Multipolar World. P.139-176.

11. Scott Charney, “Collective Defense: Applying Public Health Models to the Internet” Microsoft, 2010.

12. “Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action” DHS, March 2011

13. “APCERT Annual Report, 2013,” APCERT, http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2013(FINAL).pdf

14. “Australian Internet Security Initiative,” ACMA.au.gov, http://www.acma.gov.au/Industry/Internet/e-Security/Australian-Internet-Security-Initiative/australian-internet-security-initiative#aisi_iia

15. “Microsoft, Europol, FBI, and Industry Partners Disrupt Notorious Zero Access Botnet that Hijacks Search Results,” Blogs.Technet.com, http://blogs.technet.com/b/microsoft_blog/archive/2013/12/05/microsoft-europol-fbi-and-industry-partners-disrupt-notorious-zeroaccess-botnet-that-hijacks-search-results.aspx

16. “METRICON 9, Full Proceedings.” https://dl.dropboxusercontent.com/u/43553/METRICON-9-Full-Proceedings.pdf

17. “Join APWG,” APWG.org, accessed August 7, 2014, http://www.antiphishing.org/join-apwg/

18. “Commercial Services,” Team-Cymru.com, accessed August 7, 2014 http://www.team-cymru.com/Services/

19. “RFC 2350 Profile,” Team-Cymru.org, accessed August 7, 2014, http://www.team-cymru.org/About/rfc-2350.html

20. “Activities – ENISA,” ENISA.Europa.eu, accessed August 7, 2014, http://www.enisa.europa.eu/about-enisa/activities

21. “Mission Statement,” FIRST.org, accessed August 7, 2014, http://first.org/about/mission

22. “Bylaws of FIRST.org, Inc.,” FIRST.org, accessed August 7, 2014, http://first.org/about/policies/bylaws

23. “FS-ISAC Operating Rules,” FSISAC.com, accessed August 7, 2014 https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_2012.pdf

24. “Mission,” Shadowserver.org, accessed August 7, 2014, https://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/Mission

25. “Standards and Guidelines,” Shadowserver.org, accessed August 7, 2014, https://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/StandardsAndGuidelines

26. “Get Reports on Your Network,” Shadowserver.org, accessed August 7, 2014, https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork

27. “About Us,” US-CERT.gov, accessed August 7, 2014, https://www.us-cert.gov/about-us

28. “Traffic Light Protocol Matrix and FAQ,” US-CERT.gov, accessed August 8, 2014, https://www.us-cert.gov/tlp