Atlantic Council

BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

CONFIDENCE-BUILDING MEASURES IN CYBERSPACE

A MULTISTAKEHOLDER APPROACH FOR STABILITY AND SECURITY

Jason Healey
John C. Mallery
Klara Tothova Jordan
Nathaniel V. Youd

CONFIDENCE-BUILDING MEASURES IN CYBERSPACE

A MULTISTAKEHOLDER APPROACH FOR STABILITY AND SECURITY

Jason Healey
Director, Cyber Statecraft Initiative, Brent Scowcroft Center on International Security
Atlantic Council

John C. Mallery
Research Scientist, Computer Science & Artificial Intelligence Laboratory
Massachusetts Institute of Technology

Klara Tothova Jordan
Assistant Director, Cyber Statecraft Initiative, Brent Scowcroft Center on International Security
Atlantic Council

Nathaniel V. Youd
Active-duty Air Force Officer and Graduate Student at the Columbia University School of International and Public Affairs

Atlantic Council

NATIONAL DEFENCE COLLEGE

Atlantic Council
1030 15th Street, NW, 12th Floor
Washington, DC 20005

ISBN: 978-1-61977-069-0

November 2014

Cover designed by Eric Gehman, based on artwork by woodleywonderworks/Flickr (licensed under Creative Commons).

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The author is solely responsible for its analysis and recommendations. The Atlantic Council, its partners, and funders do not determine, nor do they necessarily endorse or advocate for, any of this report's particular conclusions. The workshops leading to this publication were sponsored by the NATO Science for Peace and Security Program, however, this publication does not represent the official views of NATO or any other affiliated organization.

NATO OTAN

This publication is supported by:

The NATO Science for Peace and Security Programme

Atlantic Council

About the Atlantic Council

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges. Founded in 1961, the Council provides an essential forum for navigating the dramatic shifts in economic and political influence that are shaping the twenty-first century by educating and galvanizing its uniquely influential, nonpartisan network of international political, business, and intellectual leaders. Through the Atlantic Council's papers and the ideas it promotes, and the communities it build, the Council's ten regional centers and functional programs shape today's policy choices and foster transatlantic strategies to advance international security and global economic prosperity.

About the Swedish National Defense College and the Institute for National Defense and Security Policy Studies

The Institute for National Defense and Security Policy Studies provides education and training for civilian and military personnel in key positions. It aims to convey a thorough understanding of Swedish and European security policy and concepts, and in the field of Swedish societal security. The Institute is an integrated part of the Swedish National Defense College, which has roots that can be traced back to its first establishment as the Artillery College at Marieberg in Stockholm during the nineteenth century. Since 2008, the Swedish National Defense College has been accredited as national university with the task of contributing toward national and international security through research and development. Research is carried out in diverse but inter-related subject areas and subsequently disseminated to other interested sectors of society, both nationally and internationally.

Acknowledgements

Special thanks to the participants at the NATO Advanced Research Workshop on Confidence- Building Measures in Cyberspace conducted on March 25-27, 2014, in Stockholm, Sweden, organized by the Atlantic Council in collaboration with the Swedish National Defense College and sponsored by the NATO Science for Peace and Security Program.

Lt. Col. *Erik Biverot*, Information Assurance and Cyber Security Coordinator, Center for Asymmetric Threat Studies (CATS), Swedish National Defense College

Vincent Boulanin, Researcher, European Studies Program, SIPRI

Raoul Chiesa, Founding Partner, Security Brokers

Laura Crespo, Political Affairs Officer, Federal Department of Foreign Affairs, Directorate of Political Affairs, Swiss Confederation

H.E. *Sorin Ducaru*, NATO Assistant Secretary General for Emerging Security Challenges

Maeve Dion, Doctoral Candidate in Law and Informatics, Swedish Law and Informatics Research Institute

Keir Giles, Director, Conflict Studies Research Center

Lt. Col. *Mikael Hagenbo*, C4ISR Officer, Swedish National Defense College

Gerd Hagmeyer-Gaverus, Programme Director and Director of Information Technology, Stockholm International Peace Research Institute

Heather Harrison-Dinniss, Senior Lecturer, International Law Center, Swedish National Defense College

John Hart, Senior Researcher, Head of the Chemical and Biological Security Project, SIPRI Arms Control and Nonproliferation Program, SIPRI

Jason Healey, Director, Cyber Statecraft Initiative, Brent Scowcroft Center on International Security, Atlantic Council

Lars Hedstrom, Executive Director, Institute for National Defense and Security Policy Studies

Mika Kerttunen, Director, Department of Leadership, Baltic Defense College

So Jeong Kim, Senior Researcher, The Attached Institute of Electronics and Telecommunications Research Institute

Alexander Klimburg, Research Fellow, Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University

Dalius Labanauskas, Head of National Security and Crisis Management, Office of the Government of the Republic of Lithuania

Gustav Lindstrom, Head of Emerging Security Challenges Program, Geneva Center for Security Studies

John C. Mallery, Research Scientist, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology (MIT)

Tim Maurer, Research Fellow, New America Foundation

Maj. Gen. (ret.) *Harold "Punch" Moulton*, Senior Director, Cyberspace Strategies, Innovation, and Consulting, Stellar Solutions, Inc.

Vardan Sargsyan, Head of the Department of Information Systems, Armenian State University of Economics

Ake Sivertun, Professor, Division of Military Technology, Swedish National Defense College

Klara Tothova Jordan, Assistant Director, Cyber Statecraft Initiative, Brent Scowcroft Center on International Security, Atlantic Council

Jack Whitsitt, Principal Analyst, EnergySec

Nina Wilhelmson, Senior Advisor, The Swedish Civil Contingencies Agency

Besir Wrayset, Crisis Management Specialist

Katharina Ziolkowski, Legal Adviser, International and Operational Law Branch, Federal Ministry of Defense, Federal Republic of Germany

The participants of the workshops that led to this report are not responsible for the contents of this publication. All final decisions on this report's contents and recommendations were made solely by the authors.

Foreword

Confidence-building measures (CBMs) try to establish practical measures between nation states to prevent and manage crises between states, based on the assumption that hostilities can occur through accident, misperception, or miscalculation. Typical examples include a "hotline" between governments or militaries or measures to improve transparency, such as exchanging visits of military officers.

Though traditional CBMs are solely between sovereign nations, in cyberspace, the actors also include various private-sector actors like the financial system, telecommunications, power grids, and energy infrastructure or critical cybersecurity and information technology companies. Each has a critical role to play in defending against cyberattacks, so the concept of CBMs must be expanded to include the private sector.

This report, which contains a number of proposed cyber confidence-building measures, is the result of discussions among participants at the NATO Advanced Research Workshop on Confidence-Building Measures in Cyberspace, conducted on March 25-27, 2014, in Stockholm, Sweden.

Sorin Ducaru, NATO assistant secretary general for emerging security challenges, welcomed participants to the workshop and outlined the current NATO cyber defense policy. The organizers of the workshop selected specific confidence-building measures out of the many discussed at the workshop for further discussion and incorporation in the final report. These specific CBMs were further discussed by participants in four working groups focusing on collaboration, crisis management, restraint, and engagement. The notes from these discussions served as the bases for this report and were further developed by the authors.

Under the leadership of **Jason Healey**, director of the Cyber Statecraft Initiative in the Brent Scowcroft Center on International Security, the Atlantic Council brought together **John C. Mallery**, research scientist at the Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory, and **Jack Whitsitt**, principal analyst at EnergySec, with the Council's **Klara Tothova Jordan** and **Nathaniel Youd** to author this report. **Lars Hedstrom**, executive director of the Institute for National Defense and Security Policy Studies, was also vital in organizing the workshop and ensuring its successful completion. **Alexander Klimburg** had the original idea and energy for the project. Special thanks to the readers who reviewed this report in its early incarnations and offered their invaluable insights and recommendations.

The confidence-building measures proposed in this publication provide a diverse set of ways to increase stability and build confidence in cyberspace without extensive legal or political action by states. Each of the measures outlined in this publication can be implemented independently, and each has varying feasibility in the current international climate.

I commend this report for further advancing a positive and practical cyber policy agenda, alongside Cyber Statecraft Initiative's numerous other issue briefs and reports.

Barry Pavel
Vice President and Director
Brent Scowcroft Center on International Security
Atlantic Council

Executive Summary

Confidence-building measures (CBMs) are an instrument of international politics, negotiated by and applied between states to strengthen international peace and security by reducing and eliminating the causes of mistrust, fear, misunderstanding, and miscalculations that states have about the military activities of other states.

But cyberspace is predominantly dominated not by the actions of states but nonstate actor. Companies and nonstate groups are the main cyber defenders and nonstate groups from hactivists to organized criminals are some of the most aggressive actors. The activities of the former group can help build trust while those of the latter can erode it. Thus, the application of concepts of CBMs appears particularly suitable for cyberspace.

CBMs must be inclusive of all stakeholders active in cyberspace. They must reduce risk and support trust by either building on preexisting concepts and mechanisms from other domains of international relations or by creating unique bottom-up approaches.

The measures proposed in this report suggest a multistakeholder-centric approach to leverage all possible stakeholders to improve overall Internet resilience and decrease the chances of miscalculation, mistrust, and misunderstanding.

This report recommends four types of CBMs that can be established to mitigate potentially escalatory effects of activities in cyberspace. These are collaboration, crisis management, restraint, and engagement measures.

Collaborative CBMs are designed to bring actors together to solve some of the unique issues in cyberspace through policing compliance with established best community practices, conducting joint international investigations into major cyber incidents to determine responsibility, and punishing offenders, much as is done under international environmental law when it comes to cross-border pollution. These CBMs rely heavily on adapting and applying existing norms and mechanisms, such as international environmental law or independent investigating bodies, to the realities of cyberspace.

The second set of proposed measures—CBMs for crisis management—focus on establishing effective communication channels for exchange of information during and following a cyber incident. The three CBMs to minimize damage during such incident involve having a functional alignment of cyber crisis response teams between different countries, establishment of a multilateral cyber hotline, and creation of an attribution and adjudication council for cyberattacks rising to the level of armed conflict. These CBMs would rely heavily on trust between nations to divulge cyber capabilities accurately and to establish a secure communication system for times of crisis. As a whole, improving crisis management measures would deter states from illegal cyber campaigns and help prevent cyber confrontations from leading to war.

To further enhance stability and confidence in cyberspace, restraint agreements between states aimed at preventing escalation of cyber activities should be implemented. Restraint CBMs built on the notion that critical entities of the Internet would be given a protected status from military-style attacks and espionage. This would work by applying international law to cyber conflicts by restricting targets for cyberattacks and establishing protected status for select critical private actors that operate the Internet.

The final set of CBMs focus on the engagement of neutral activists and adaptation of technical norms in cyberspace to support the stability of the Internet. These two CBMs present methods to engage nongovernmental organizations to increase stability in cyberspace and work to establish norms and standards for cyber actions. This would start a grassroots movement, engaging researchers collaborating on transnational issues. Through leveraging all actors' skills, it would protect and support vital elements of cyberspace. Further, by bringing together a diverse set of organizations, they are able to collaborate to address minor cyber incidents and help states share information in a transparent manner.

The four types of proposed CBMs would allow states to address those cyber activities that take place well below threshold of "armed conflict" and do not constitute normal politico-military risk reduction tactics. These measures would create new avenues to confidence-building in cyberspace that uses a bottom up approach to norms of behavior, aided by multi- and bilateral state-to-state actions and support.

These CBMs, each of which can be implemented independently, are designed to provide a diverse set of multistakeholder ways to increase stability and build confidence in cyberspace without extensive legal or political action by states.

Table of Contents

Introduction 1

1. CBMs for Collaboration 3

2. CBMs for Crisis Management 7

3. CBMs for Restraint 13

4. CBMs for Engagement 16

Conclusion 19

Introduction

Confidence-building measures (CBMs) are an instrument of international politics, negotiated by and applied between states.[1] CBMs aim to prevent the outbreak of an international armed conflict and accidental escalation by virtue of establishing practical measures and processes of preventive crisis management between states.[2]

The ultimate goal of CBMs is to strengthen international peace and security by reducing and eliminating the causes of mistrust, fear, misunderstanding, and miscalculations that states have about the military activities and intentions of other states. CBMs help to prevent military confrontation as well as covert preparations for the commencement of war, and reduce risk of surprise attacks and of the accidental outbreak of war.[3]

Although originally drafted in the context of disarmament, CBMs can reduce the chances of conflict in cyberspace as well.[4]

In the field of conventional arms, CBMs include information exchange measures, observation and verification measures, and military constraint measures. CBMs can be formal or informal, unilateral, bilateral, or multilateral, military or political, and can be state-to-state or nongovernmental. Oftentimes, CBMs appear in legally binding agreements.

Due to the nature of the Internet, the scope and potential consequences of malicious cyber activities, such as espionage and cybercrime, can easily lead to escalation. Their potency, low cost, and potential deniability make them especially counterproductive to building trust.

Additionally, complexity induced by varying vocabulary between states in describing activities in cyberspace, differences in actors' concepts of red lines and attribution and verification challenges all contribute to the need for CBMs.

The "borrowing" of the concept from a traditional, nonproliferation context for cyberspace has its limits. CBMs in conventional arms domain are built on monitoring and verification mechanisms, whereas monitoring and verification are difficult to implement in cyberspace.

Anonymity, complexity, the intangible nature of digital systems, and the lack of knowledge about the intended use of hardware and software make any verification often not technically practicable or politically feasible, thus precluding, at least in a short term, legally binding agreements patterned on traditional arms control. Yet there is an important role for CBMs in reducing risk and building trust through measures that enhance transparency, cooperation, and stability.

A number of steps have been taken by international organizations such as the United Nations (UN)[5] and the Organization for Security and Cooperation in Europe (OSCE) to develop such measures for cyberspace.[6] The initiatives within the OSCE are expressions of political will to share information on a range of different cyber-related matters.

All of these initiatives closely mirror other measures employed in the disarmament area. They include actions of states, on voluntary basis, to provide national views on aspects of national and transnational threats to and in the use of information and communications technologies (ICTs). These initiatives facilitate cooperation among the competent national bodies, exchange information in relation with the security of and in the use of ICTs, encourage consultations in order to reduce the risks of misperception of cyber activities, provide a list of national terminology relating to ICT security, and provide contact data of existing national structures that manage ICT-related incidents, and coordinate responses.

States are not the only, or even necessarily the most important, actors in cyberspace. The role of companies, nongovernmental organizations, civil society, and others increases the scope for far more CBMs that do not fit the traditional model of state-based CBMs but which nonetheless could strengthen transparency and confidence.

1 CBMs are also known in their advanced forms as "transparency and confidence-building measures" or "confidence-, transparency- and security-building measures."

2 Katharina Ziolkowski, *Confidence-Building Measures for Cyberspace—Legal Implications*, (Tallinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence, 2013).

3 Guidelines for appropriate types of confidence-building measures and for the implementation of such measures on a global or regional level, prepared by the United Nations (UN) Disarmament Commission's Consultation Group in 1988.

4 Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO Cooperative Cyber Defense Center of Excellence, 2013).

5 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations General Assembly Study Series 33, UN Doc A/68/98, June 24, 2013, reissued for technical reasons on July 30, 2013; Center for Strategic and International Studies, Institute for Peace Research and Security Policy, and United Nations Institute for Disarmament Research, *The Cyber Index: International Security Trends and Realities*, (New York and Geneva: UNIDIR, 2013), http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf.

6 "Decision No. 1106 Initial Set of OSCE Confidence-Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies," PC.DEC/1106, Organization for Security and Cooperation in Europe, December 3, 2013.

A multistakeholder model, inclusive of state and nonstate actors, is likely the most effective model of collaboration to ensure the stability and security of the Internet.

CBMs and NATO

NATO's 2010 Strategic Concept linked cyber issues to the core of NATO's business. The Alliance's focus in the area lies in the defense of its own infrastructure and capacity building of allied nations. In parallel, NATO's core purpose is promotion of cooperation on defense and security issues to build trust and, in the long run, prevent conflict in all domains, including cyberspace.

In line with the nonduplication principle, NATO's mandate in CBMs is limited to monitoring the evolution of rules in the area and supporting the development of national efforts. Since NATO is a group of "like-minded" nations, it has not traditionally served as a platform for development of CBMs.

Nevertheless, because cyber topics cover a wide range of activities, including areas like crime and espionage, disagreements arise even between close allies. As a result, NATO might indeed be a place to nurture cyber CBMs. Moreover, individual efforts of member states to elaborate and adopt CBMs would, in the long term, strengthen international peace and security.

NATO could play a more active role with respect to CBMs and can shape the discussion and debate. It could publicly promote the ideas of confidence-building in cyberspace and publicly subscribe to rules of behavior supportive of stability and collaboration in cyberspace.

Specific CBMs in Cyberspace

This report outlines four types of CBMs that can be established to support stability and trust regarding state activities in cyberspace: collaboration, crisis management, restraint, and engagement.

The first set of CBMs is designed to bring actors together to solve some of the unique issues in cyberspace. The three collaboration CBMs this report outlines include policing compliance with established best community practices, conducting joint international investigations into major cyber incidents to determine responsibility, and applying concepts from international environmental law to cyberspace.

The second set consist of collaboration CBMs including crisis management measures that focus on how to communicate during and following a crisis. These CBMs aim to allow the vested actors in cyberspace to communicate effectively to resolve cyber crises. This report outlines three crisis management CBMs: functional alignment of cyber crisis response teams; a multilateral cyber hotline, which would enable state to state communication during a crisis; and a multilateral cyber adjudication and attribution council, which would provide attribution support to states that do not have the technical capabilities to do it unilaterally.

The third set of CBMs focus on restraint of action in order to maintain system-wide stability. The two restraint CBMs include restrictions on target selection, which would protect vital entities during peacetime, and applying legal or political neutrality status to select cyber "safe havens" before and during a conflict.

The final set of CBMs focus on engaging a diverse set of actors to increase stability and build confidence. The two engagement CBMs include creating an organization to allow technically skilled and nonaffiliated individuals and actors to use their knowledge to protect important parts of cyberspace and using technical regimes to establish political as well as technical norms and standards in cyberspace.

The ultimate goal of CBMs is to strengthen international peace and security by reducing and eliminating causes of mistrust, fear, misunderstanding, and miscalculations.

1. CBMs for Collaboration

This section outlines three specific CBMs that a diverse group of cyber stakeholders can implement in the next several years. These multistakeholder centric CBMs include policing compliance with existing best community practices (BCPs) in cyberspace, conducting joint investigations following major cyber incidents, and applying the environmental law model in cyberspace.

These three CBMs present several multistakeholder centric methods to ensure the diverse skills, talents, and resources of the various actors in cyberspace are appropriately leveraged to increase overall confidence in cyberspace.

Policing Best Practices

Objective and Scope

In the past several years, the international community has established many BCPs for cyberspace. Unfortunately, many BCPs are ignored, and this is one of the major factors that contributes to distributed denial of service (DDoS) and other attacks. Today, the challenge is enforcing existing BCPs rather than establishing new ones.

Two high profile examples of this problem include BCP 140[7] on recursive DNS servers or BCP 38[8] on the need for Network Ingress Filtering.[9] BCP 38 was adopted in May 2000 but little progress has been made in establishing and enforcing practices to use ingress traffic filtering to prohibit DDoS attacks. This CBM would establish a group to assess which organizations are adhering to existing BCPs and which are noncompliant. This group would then contact violators in order to give them a chance to comply with the BCP before publicizing their lack of compliance.

Actors

The specific CBM would be the formation of an organization to "police" best practices. Such an organization could be created by a single state, between like-minded states, or even by companies or nongovernmental organizations.

The implementation of this CBM involves three main sets of actors: funders, staff, and violators. The funders and other stakeholders that enable this CBM include nongovernmental organizations, international organizations, and governments. The personnel of this new organization would include a secretariat, staff, and other senior advisers with the technical and legal expertise necessary to determine compliance with existing BCPs. Violators include all network providers and others that currently ignore the existing BCPs.

Implementation

This CBM centers on the agreement of states to create a process for adhering to and codifying existing norms. It will utilize existing organizations including the Internet Engineering Task Force (IETF), the Internet Society (ISOC), and the World Wide Web Consortium (W3C) and can draw talent from existing semi-volunteer groups, such as I Am the Cavalry, to pool talent and technical expertise.

A budget of several million dollars would be sufficient to create a small team able to fulfill the group's mission. Possible funders include governments, interested corporations, industry groups, and high-net worth individuals.

The team would first establish a measurement process to determine which organizations are complying with the existing BCPs and which are not. This process would include a protocol for contacting violators giving them a chance to comply with the relevant BCPs. If the organizations fail to comply, the group would then implement a naming-and-shaming process to expose repeat violators and encourage future compliance.

Establishing this group to police BCPs would require a strong multistakeholder process. If existing organizations and governments support establishing such a group, it could be implemented inexpensively and in a relatively short period of time.

On a state-to-state level, the state parties would establish an inter-agency working group at the ministerial level to develop a common understanding of the need to establish a group to assess which organizations are adhering to the existing BCPs, informed by and with contributions from relevant national and international nongovernmental organizations. Additionally, states, with help from the nongovernmental sector, would nominate potential members of the group. The group would convene for the first time six months after the conclusion of the CBMs and would continue its work on a basis of regular meetings at intervals to be agreed.

7 BCP 140 is Internet best current practice preventing use of recursive name servers in reflector attacks. Network Working Group, Internet Engineering Task Force, "Preventing Use of Recursive Nameservers in Reflector Attacks," https://tools.ietf.org/html/bcp140.

8 BCP 38 is Internet best current practice on defeating denial of service attacks that employ IP source address spoofing. Network Working Group, Internet Engineering Task Force, "Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing," http://tools.ietf.org/html/bcp38.

9 Ibid.

Feasibility

A major concern is the effectiveness of such a naming-and-shaming campaign. It may be difficult to encourage violators to change their behavior short of a stronger enforcement organization if naming and shaming is ineffective. However, even if naming and shaming does not succeed in changing organizations' behaviors, such a campaign would still be more effective than ignoring the issue and allowing current violators to continue to operate without exposure.

Joint Investigations into Major Cyber Incidents

Objective and Scope

This CBM is modeled after the Joint Investigation Group that examined the attack against South Korean ship *Cheonan*.[10] This investigation was conducted by a multinational committee with experts in different fields to determine the cause of the *Cheonan*'s sinking. The group examined forensic evidence of the explosion, including a fragment of a torpedo found nearby, and established North Korea's culpability for the ship's sinking.

Following a major cyber incident, determining who was responsible for the incident is important in order to maintain stability and avoid escalation. This CBM would establish a mechanism to form an ad hoc group of technical experts following a major incident to conduct an international investigation into all evidence and determine which nations or nonstate actors were responsible. Such evidence would include all technical data as well as other pertinent information that could aid the investigation.

Actors

The specific CBM would be a commitment of state and nonstate actors to work toward the common understanding of the need to endeavor creation of joint investigation process. This would be followed by the establishment, on a state-to-state level, of an inter-agency working group that would designate a list of individuals to participate in this multinational effort.

This group would consist of individuals with the expertise needed to investigate the specific incident. As the group would be established ad hoc following an incident, it is difficult to determine who would participate ahead of time, but standards can be established before an incident to ensure that the group includes individuals with the appropriate expertise and

The rapidly increasing connectivity and reliance of cyberspace has not been matched by equally expeditious development of norms and rules that would govern the behavior of stakeholders involved in its use.

represents significantly diverse technical and political backgrounds, with other experts who are able to understand all aspects of the event. The group should be chaired by an independent and well-respected individual who will be seen as neutral.

Implementation

The cyber investigations group could be convened by requesting governments or could be organized solely by the technical community. The team should include independent international professionals and be chaired by an independent and well-respected person in order to maintain the group's impartiality and credibility.

The investigations conducted by the group should use a standard analytical framework, such as the spectrum of state responsibility, to draw data-based conclusions.

The success of the group's early investigations will help determine its future standing. If it is successful in early investigations, its status could grow over time into a standing independent multistakeholder body.

Feasibility

Establishing this group to conduct joint investigations would require a strong multistakeholder process. Its work will be contingent on the occurrence of major

10 *Joint Investigation Report: On the Attack Against ROK Ship Cheonan* (Ministry of National Defense, Republic of Korea, September 2010), http://old.armscontrolcenter.org/policy/northkorea/articles/cheonan%20investigation%20report_1.pdf.

cyber incidents. However, if existing organizations and governments support forming such a group, it could be implemented inexpensively and in a relatively short period of time.

The group's work could face opposition by governments that want to retain and use secret cyber capabilities. Even governments not under investigation could block the work of the group in order to protect their cyber capabilities from public exposure.

International Environmental Law Model[11]

Objective and Scope

The rapidly increasing connectivity and reliance on cyberspace has not been matched by equally expeditious development of norms and rules that would govern the behavior of stakeholders involved in its use.

International law has been successful in creating regimes that govern many aspects of international relations. Varying legal and political frameworks have been applied to cyberspace, the most common being technical, criminal, and warfare norms. None have succeeded, for the time being, in achieving the desired stability in cyberspace, and they have mostly been outpaced by proliferating cyber threats. However, most of the frameworks are fairly new, and their effectiveness will be tested in the years of implementation.

A potentially promising framework that would address these challenges could be based on international environmental law. This framework cannot replace other elements needed for secure and stable Internet; it will not invent more secure technologies, defeat cyber criminals, or help militaries understand the laws of armed conflict in cyberspace.

However, applying environmental legal norms to cyberspace could be useful because much of international environmental law addresses a problem familiar to cyber policymakers—the inherent tension between a state's sovereignty and its obligations to individuals, other states, and a shared common space. As nations analyze their environmental rights and responsibilities under international law, they will find many concepts that are also applicable to cyberspace.

Actors

The specific CBM would first involve multistakeholder parties working toward a common understanding of the need to apply the environmental model to governance of cyberspace, followed by a commitment of states to work toward a common understanding of the need to define norms for the cyberspace built on concepts from environmental law.

The analogy between harm to physical environment is quite fitting to the cyber-environment. For instance, denial of service attacks, spam, and other Internet ills can be thought as "pollution" of the environment of cyberspace.

Internet Service Providers (ISPs) then could be seen as originating or passing along pollution by not cracking down on botnets (computers compromised and under automated control of hackers) in their networks and not filtering the attacks out of their traffic flow. Nations could be seen as passively allowing the ISPs to pass along this pollution by not having sufficiently strong laws or regulations to restrict its flow.[12]

To tackle these challenges, states and nonstate actors could agree on a set of basic norms such as:

- *Good Stewardship*: Increasingly people want to be stewards of the environment, to keep it clean for their own purposes, for others who depend on it as a resource, and even for the use and enjoyment of future generations. Just as the international community works to ensure environment sustainability, it should work to ensure the sustainability of cyberspace.
- *Accountability for Cross-Border Pollution*: According to the results of the International Joint Commission's Trail Smelter decision,[13] which settled a long-standing dispute between Canada and the United States, states can be liable for harm from cross-border pollution. The definition of pollution might usefully be broadened to include "emissions" like spam or botnet attacks.
- *Use but with Limits*: According to Principle 21 of Stockholm Declaration[14] (a generalization of the Trail Smelter decision), states have sovereign use of their own natural resources but also a responsibility to not cause damage outside that jurisdiction. If the idea of resources expanded to include computers and networks, this concept could easily apply to cyberspace.[15]

11 Jason Healey and Hannah Pitts, "Applying International Environmental Legal Norms to Cyber Statecraft," *I/S: A Journal of Law and Policy for the Information Society* 8, 2012, p. 357.

12 For the Analysis and Identification of P2P Botnet's Traffic Flows, see Wernhuar Tarng, Li-Zhong Den, Kuo-Liang Ou, and Mingteh Chen, "The Analysis and Identification of P2P Botnet's Traffic Flows, *International Journal of Communication Networks and Information Security (IJNIS)*, vol. 3, no. 2, August 2011, http://www.ijcnis.org/index.php/ijcnis/article/viewFile/79/75.

13 Trail Smelter Arbitration Case 1941, UN Rep. Int'L Arb. AWARDS 1905 (1949).

14 Declaration of the United Nations Conference on the Human Environment, UN Doc. A/Conf.48/14/Rev. 1(1973); 11 ILM 1416 (1972).

15 For more on the applications of these norms, see Jason Healey and Hannah Pitts, "Applying International Environmental Legal Norms to Cyber Statecraft," *I/S: A Journal of Law and Policy for the Information Society*, 2012.

Implementation

At the international level, nations share long-standing traditions by which they cooperate toward the ends of international security. International organizations have had some success with creating norms for some of the aspects of interactions in cyberspace.

Most importantly, environmental norms have not been created just by government action, but also by individuals (think Rachel Carson), local, and international civil society groups, corporations (such as by building LEED-certified buildings or certified sustainable fish or lumber). Best of all, these norms demand local action but are still international in applicability and are strongest in the digital generation.

States and nonstate actors should therefore push the idea of a clean Internet,[16] free from polluting attacks, and supporting norms and CBMs.

A wider system of governance comprising a set of multi-stakeholder organizations, including the Internet Society (ISOC), Internet Engineering Task Force (IETF), could support states in developing the indicators of "pollution" and other technical elements that would indicate the breach of the norm.

Feasibility

Two potential blockers for success of the measure are the disagreement between states on how international law applies to cyberspace and diverging views of the need to establish norms for cyberspace between nations.

In the trinity of the goals of CBMs—transparency, stability, and cooperation the collaboration measures would contribute foremost to the stability and transparency of interstate cyber relations by reinforcing the collaboration between state and nonstate actors globally in assuring that minor cyber incidents do not escalate and states share information in a transparent manner.

The analogy between harm to physical environment is quite fitting to the cyber-environment. For instance, denial of service attacks, spam, and other Internet ills can be thought as "pollution" of the environment of cyberspace.

16 Concept similar to clean pipes initiative aka packet staining, Tyson Macaulay and Chris Mac-Stoker, "Delivery Options for Upstream Intelligence, *Anewsletter*, vol. 13, no. 4, fall 2010, https://www.bell.ca/web/enterprise/newsRoom/en/pdf/Delivery_Options_for_Upstream_Intelligence.pdf?EINT=rclanding_en_sol.

2. CBMs for Crisis Management

Cyberspace today reflects the actions of governments, corporations, individuals, and many other actors. Stability in cyberspace requires cooperation of actors relevant to an issue within a multistakeholder approach.[17]

This section outlines three CBMs to increase stability during cyber crises by enhancing crisis communication and by providing mechanisms for managing cyber disputes. These CBMs are functional alignment of cyber crisis response teams between different countries, establishment of a multilateral cyber hotline, and creation of an attribution and adjudication council for cyberattacks rising to the level of "armed conflict."

The international relations literature on crisis management[18] tends to focus on political-military crises, where the risk of serious escalation or war is imminent. Few analysts believe that pure cyber conflicts are possible or doubt that cyber crises are not embedded within broader politico-military disputes.[19] For the purposes of this report, a *cyber crisis* refers to those dimensions of a politico-military crisis involving risks to computation and networking underpinning national security or major components of national economies. Distinct treatment of the cyber dimensions of crises is warranted because the technical and socio-technical aspects of cyber interactions bring to traditional concepts of politico-military crises new expertise, new actors, new organizational forms, and compressed time scales. Moreover, future cyber crises, will likely take on characteristics resembling financial crises to the extent that cyberattacks directly disrupt systemically important financial systems, indirectly disrupt them through telecom or power outages, or significantly undermine confidence in them through information operations. Over time, the cyber dimension will become fully integrated in thinking about politico-military crises under conditions of informationized societies and globalized ICT interdependence.[20]

The discussion in this section contemplates cyber crises as conflict reaches thresholds of war. But, it recognizes the possibility of contagion from lower intensity cyber operations, like prepositioning of "logic bombs" in critical infrastructure, which can quickly escalate into national security crises.

Functional Alignment of Cyber Crisis Response Teams

Objective and Scope

Cyber crisis response teams around the world may encounter difficulties communicating with each other due to the differing organizations structures and functional roles across countries. This CBM will assure that cyber crisis response teams can identify, access, and exchange data with their functional counterparts in other states to manage the various aspects—political, military, economic—of cyber crises.

At the bilateral level, this CBM focuses on developing interstate contacts between functional counterparts. At the multilateral level, it develops a functional directory to realize the same purpose for cyber crises involving a broader set of states. The objective is to enable the right people to communicate quickly to share situational awareness whether they are direct or indirect parties to the crisis. For best results, states contemplating crisis communications with specific counterparts should engage proactively and conduct exercises to test the capability.

Actors

Engagement would involve a foreground of state-to-state contact but would naturally include crosscutting contacts with relevant private sectors. State engagement would focus on the national security, military intelligence, and homeland defense components. Additional engagement would involve sectoral cyber defense entities and operators of key critical infrastructure such as power, telecommunications, finance, and energy sectors. The private sector engagement could also include the cybersecurity industry and relevant vendors of ICT products or services.

17 The section on conflict management was improved by comments by Brian David Mussington, Catherine B. Lotrionte, and William Studeman, but responsibility for errors or omissions falls to the author, John C. Mallery. John C. Mallery's contribution was part of research conducted at the Computer Science and Artificial Intelligence Laboratory of the Massachusetts Institute of Technology, whose research is supported in part by the Office of Naval Research Grant N000141310878 and the Department of Defense Minerva Research Initiative.

18 Some examples for political science include: Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. (New York: Longman, 1999); Lincoln P. Bloomfield and Allen Moulton, *Managing International Conflict: From Theory to Policy: A Teaching Tool Using CASCON*, (New York: St. Martin's Press, 1997); Joseph S. Nye Jr., "Nuclear Lessons for Cybersecurity," *Strategic Studies Quarterly*, winter 2011; Stephen J. Cimballa, "Nuclear Crisis Management and 'Cyber War' Phishing for Trouble?" *Strategic Studies Quarterly*, spring 2011; John C. Mallery, "Crisis Management Under Informatization: Confidence and Security Building Measures for Escalation Control," invited presentation at the Eighth International Forum: State, Civil Society and Business Partnership on International Information Security and the Ninth Scientific Conference of the International Information Security Research Consortium, Garmisch-Partenkirchen, Germany, April 21-24, 2014; Paul K. Davis, "Deterrence, Influence, Cyberattack, and Cyber War," Working Paper WR-1049, RAND, June 2014.

19 This view is held by both Russian and US cyber strategists, personal communication, 2011-2013.

20 Russia's annexation of Crimea and support for secessionists in eastern Ukraine provide a new exemplar of cyber blended into pol-mil crisis as telecom infrastructure was subverted for military gains and propaganda was deployed to undermine resistance. The Ukrainian case is driving NATO assessment of its posture to handle future crises. Robin Niblett, "NATO Must Focus on 'Hybrid Wars' Being Waged on the West," *Financial Times*, July 17, 2014.

Implementation

Each state would be responsible for maintaining an index of expertise and authorities responsible for functional areas where a cyber crises may develop. The index would also include contact information and relevant protocols for data exchange within the functional area. For cyber threat analysis, standardized protocols and formats are gaining broader acceptance. For example, the Trusted Automated eXchange of Indicator Information[21] (TAXII) provides transport mechanisms for exchange of cyber threat intelligence using Structured Threat Information eXpression[22] (STIX).

The effectiveness of the directory would be tested periodically through exercises based on plausible scenarios across various critical cyber domains, and would range from political and military threats to incidents involving critical infrastructure. Scenario driven gap analysis would be used to identify areas for improvement.

The indexes would be updated for personnel turnovers, organizational changes, or evolution of data exchange protocols as they occur. A taxonomy of functional areas that span the participating countries would be updated based on an initial functional survey and subsequent scenario based induction. All participating states would be advised to use the standard functional taxonomy as it pertains to their national situations.

If directory scaling becomes a concern, these directories could be represented as description logics (aka semantic web) which are computationally tractable and complete. This would enable fast subsumption reasoning to determine responders and ability to support interoperable directories and functionally based messaging.

The specific CBM would be a commitment of states to work toward a common understanding of the need to fully develop escalation contacts, including procedures, data exchange protocols, and tools to operationalize functionally indexed directories. This would be followed by establishment, on a state-to-state level, or an inter-agency working group that would develop the list of escalation contacts.

States would work to establish, initially through bilateral agreements between major powers, a list of shared contacts. At the beginning, this effort would initially focus on members of the OSCE. It could eventually expand to include other multilateral and regional organizations such as the Association of Southeast Asian Nations (ASEAN), Organization of American States (OAS), and the African Union (AU).

When a cyber crisis involving participating states arises, the needed correct mix of responders and interlocutors could be looked up by expertise and authority in a directory indexed by functional domains.

Hotlines for crisis management are more useful if the counterparty is relevant for the task at hand. By maintaining a directory of functional expertise and responsibilities, a state can quickly match the people and organizations to the crisis at hand. As the CBM does not require prior disclosure, states should be more willing to create and maintain a directory of relevant individuals. Exercises around scenarios designed to test crisis response in functional areas can be negotiated to avoid exposure of sensitive personnel or organizational information.

Feasibility

States may be reluctant to divulge some cyber crisis response teams because they wish to protect sensitive functional areas. For instance, states may not want to disclose the cyber resilience of nuclear weapons systems or other highly sensitive capabilities. As this CBM does not necessarily require prior foreign disclosure of personnel, states should be more willing to create and maintain an internal directory of relevant individuals for access via index terms during a crisis. Furthermore, states may not want to expose exactly how they are organized so that they appear more or less capable than they actually are, depending on their security concerns. Similarly, exercises around scenarios designed to test crisis response in functional areas can be negotiated to avoid disclosure of sensitive personnel or organizational information. Of course, priorities and available budgets will constrain the willingness of states to participate in exercises or elaborate preparations.

Compiling and maintaining a working directory may be difficult due to evolving cyber terrain and changing socio-technical capabilities. By the time a complete directory is established, it may be outdated due to personnel change and the evolution of organizations. Finally, organizing cyber crisis response teams by functional roles may be difficult without disclosing sensitive concepts and methods. For example, states may be unwilling to share pre-delegated authorities for cyber responses or targeting for cyber operations in order to preserve potential for operational surprise.

If states can overcome these concerns they should be able to develop an initial working directory quickly for minimal cost. States should be able to implement an initial version of this CBM in six to eighteen months.

21 Julie Connolly, Mark Davidson, and Charles Schmidt, "The Trusted Automated eXchange of Indicator Information (TAXII)," Mitre, May 2, 2014.
22 Sean Barnum, "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIXTM)," Mitre, February 20, 2014.

Hotlines for crisis management become more effective when the appropriate counterparties can be readily accessed and necessary data exchange infrastructure is in place. The availability of these directories of functional expertise and responsibility enables timely convening of the people and organizations best suited to manage the crisis at hand, and thereby, enhances the effectiveness of hotlines.[23]

Multilateral Cyber Hotline Initiative

Objective and Scope

At the onset of a cyber crisis, secure and reliable communication between national command authorities is essential to manage, deescalate, and resolve the crisis. During a cyber crisis, traditional communication channels may be compromised or inoperative. As a result, it is important to establish a secure and resilient communication channel or a hotline that will function during and following a cyber crisis.

Actors

The specific CBM would be a commitment of states to work toward a common understanding of the need to establish a multilateral cyber hotline initiative. This would be followed by establishment, of a state-to-state level, or an inter-agency working group to negotiate the implementation details for the hotline.

Implementation

Establishment of a cyber hotline has already been undertaken by the United States and Russia,[24] and has been raised in discussions between the United States and China.[25] Implementation of additional hotlines should continue starting among states belonging to the OSCE and the OSCE itself. As experience is gained, ASEAN, OAS, AU, and other regional organizations may decide to establish cyber hotlines for their member states.

This hotline CBM would initially focus on bilateral state interaction but could be subsequently expanded to include secondary parties and to multilateral contexts in regional organizations. The aim is to ensure that appropriate actors are convened over reliable communications links to create shared situational awareness and to manage the specifics of a cyber crisis.

The OSCE already provides a secure communications infrastructure over which member states communicate with each other. This infrastructure can be reinforced to offer survivable hotline links among members during a cyber crisis. Hotline procedures should be developed to specify not just operational mechanics but also provide templates and data exchange formats for anticipated cyber problems in areas like critical infrastructure, core economic activities, or military interactions. Voice, text, multimedia, and data exchanged over a hotline must be captured and available for recall by both parties in order to assure accurate translation and interpretation, even if, under special circumstances, states may wish to suspend non-reputability. To ensure that the hotline infrastructure can be used effectively and without delay during a crisis, advance preparation must establish and exercise operational procedures with relevant points of contact and simulated data exchanges.

This hotline CBM enables the national command authority of a state to communicate with its counterpart during a crisis in order to reduce tensions, correct misunderstandings, and avoid miscalculation.

Hotlines are important to help manage cyber crises when they arise. Yet, building bilateral connectivity among all state dyads would involve major duplication of effort. For the case of OSCE with fifty-seven members, a complete communications hub would require the equivalent 1,596 bilateral links.[26] Consequently, it is more efficient to create a shared architecture that makes best practices and high security engineering available to all. In addition, technical guarantees concerning the availability, integrity, and confidentiality of this shared crisis communications infrastructure would increase its acceptability, as would some successful use cases. Moreover, selection and implementation data exchange standards would enhance the ability to create shared situational awareness during the height of crises. Finally, because they also rely on it, member states would have incentives to protect the infrastructure, including the networking and computing components, whether physical or logical. Even greater confidence in the infrastructure can be inspired by proscribing attacks on the hotline infrastructure under international law.

An important survivability baseline for the hotline infrastructure is the ability to resist attacks by nonstate actors, or, at a minimum, recover rapidly. Periodic exercises can ensure that states understand how to utilize the infrastructure. Also, such exercises would test the survivability of the infrastructure under evolving actor cyber capabilities and would build confidence in the ability of states to communicate effectively during times of crisis.

23 OSCE rules 8 and 3 cover CBMs that would reach similar goal. Decision No. 1106 Initial Set of OSCE confidence-building measures to reduce the risk of conflict stemming from the use of information and communication technologies. PC.DEC/1106, December 3, 2013.

24 White House, Office of the Press Secretary, "FACTSHEET: U.S.-Russian Cooperation on Information and Communications Technology Security," June 17, 2013, http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

25 The United States briefed China on its cyber hotline agreement with Russia and discussed the prospect of developing one between the United States and China during a track 1.5 dialogue in June 2013.

26 Such a communications hub forms a complete graph and, therefore, the duplication of effort asymptotes to $N(N-1)/2$ where N is the number of connected national commands.

Feasibility

Some impediments to implementing a multilateral communications infrastructure include state concerns about the security of communications. States may doubt the ability to communicate confidentially with other states over the infrastructure without third parties intercepting their communications. Confidentiality may be assured by using high assurance systems, deploying transparent and verifiable designs, enforcing supply chain integrity, and providing user selectable cryptographic algorithms and keying schemes.

States may also be reluctant to rely on multilateral hotline hubs for communications with peers due to fear of catalytic attacks against the communications infrastructure by third parties intending to exacerbate the conflict.

If states are willing to adopt a reinforced OSCE infrastructure for cyber crisis communication, an initial implementation could become operational in six to eighteen months.

Multilateral Cyber Adjudication and Attribution Council

Objective and Scope

One of the primary difficulties in resolving cyber disputes is attributing attacks to the perpetrator. The Multilateral Cyber Attribution and Adjudication Council (MCAAC) would provide an international mechanism for arriving at a consensus attribution of illegal cyber campaigns by states and a formal process for adjudicating associated interstate disputes.

Actors

This specific CBM involves a commitment of states to develop an understanding of the need for MCAAC and the path for its determinations and judgments to be perceived as legitimate. Given the commitment, a working group representing states would develop the framework for creation and operation of such attribution and adjudication body.

Currently, states' ability to attribute malicious cyber activity varies depending on their cyber capabilities and other elements of national power. The MCAAC can help raise the expected attribution for states with lower attribution capacity by leveraging that of advanced cyber powers and cross-correlating a mosaic of elements leading to attribution of illegal cyber activity.

Once a cyberattack or campaign has been identified and attributed, the MCAAC can also recommend steps to de-escalate the dispute or refer the case to a specialized conflict manager. There are various precedents from counterterrorism[27] and the Biological Weapons Convention (BWC) for how MCAAC might operate but the activities of the International Atomic Energy Agency (IAEA) under the Nuclear Nonproliferation Treaty (NPT) are most germane.[28]

The MCAAC must focus on cyber campaigns that are illegal[29] under international law. Under international law, cyber operations are illegal when they rise to the level of "armed attack" or "use of force." Under International Humanitarian Law,[30] cyber operations are illegal when they adversely affect civilian or noncombatant populations, for example, violating the principle of distinction or attacking protected entities or personnel. Other areas of customary international law or trade law, such as World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS),[31] may come into play when they proscribe cyber operations that wrongfully harm another state or violate treaty commitments to refrain from theft of intellectual property for commercial gain.

Any state could refer a cyber incident or campaign to the MCAAC for investigation or adjudication based on probable violation of relevant international law by another state or its proxy. If a plaintiff already has attribution evidence, it may seek only adjudication.

Implementation

The council's investigation capabilities would mostly come from states with higher cyber attribution and forensics capacities. Some possible states that have the relevant capabilities include the United States, the United Kingdom, France, the People's Republic of China, and Russia.

When a cyber incident or campaign is brought to it, the MCAAC would seek attribution information for the case from member states, security companies, telecommunications providers, and others. It would integrate the evidence to produce an attribution report for the case. When attribution is high confidence, the defendant state would be given an opportunity to present exculpating evidence and arguments. MCAAC

27 Richard J. Aldrich, "US–European Intelligence Co-operation on Counter-Terrorism: Low Politics and Compulsion," *The British Journal of Politics & International Relations,* vol. 11, no. 1, 2009, pp. 122-39.
28 Simon Chesterman, "Shared Secrets: Intelligence and Collective Security," Lowy Institute Paper 10, 2006; For a more broader treatment of intelligence sharing, see Born, Hans, Ian Leigh, and Aidan Wills, eds., *International Intelligence Cooperation And Accountability* (Oxford: Routledge, 2011).
29 Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law*, vol. 37, 1999. Michael Schmidt, ed., *op cit.* discusses when a cyber action or campaign rises to the level of "armed conflict" or violates international humanitarian law.
30 Jean-Marie Henckaerts, Louise Doswald-Beck, and Carolin Alvermann, eds., *Customary International Humanitarian Law, Volume 1:Rules* (Cambridge: Cambridge University Press, 2005).
31 Agreement on Trade-Related Aspects of Intellectual Property Rights, World Trade Organization, Marrakesh, Morocco, April 15, 1994.

would then weigh the evidence and rule on the case. Where the defendant is found responsible, MCAAC would issue a recommendation on steps to deescalate the malicious activity. The MCAAC could also rule on damages to be paid to the plaintiff by the defendant as compensation.

If an attribution ruling finds against the defendant, the MCAAC would refer the case along with the evidence and its recommendations to the United Nations Security Council (UNSC), the International Court of Justice (ICJ), or a regional security body, as appropriate. If accepted, that body could resolve to undertake enforcement action. Thus, the MCAAC could become a specialized advisory agency for cyber violations of international law that formalizes and institutionalizes cyber attribution and adjudication. It would gain legitimacy through technical competence, the impartial professionalism, and the authority of the UNSC, ICJ, or regional security bodies that would serve as enforcers.

States can refer a cyber incident or campaign to the MCAAC. When the impact is determined to cross a threshold for the relevant area of international law, MCAAC would then investigate and, if feasible, arrive at positive attribution for authorship. If the MCAAC is unable to attribute responsibility for the incident, it would report and preserve the available evidence for possible future use should the case be revisited in light of new information. When attribution is possible, then MCAAC should recommend steps to deescalate the cyber dispute and possibly render a judgment that assigns costs for the repair of damage to the aggressor.

Operation of MCAAC depends on the ability to determine that a cyber incident or campaign reaches a threshold of "armed attack," where a state is entitled to self-defense or at least the lower threshold of "use of force,"[32] as defined by Article 2(4) of the UN Charter and assign state responsibility for "effective control" or at least "overall control."[33]

Whether a cyber incident or campaign reaches thresholds for "armed attack" depends, according to the Tallinn Manual, on the "scale and effects" based on severity, military character, state responsibility, directness, invasiveness, immediacy, and measurability.[34] The key criteria is severity of effects, which refers to physical harm to persons or property or "grave impact" on critical national interests. The lesser threshold of "use of force" remains subject to considerable debate but involves cyber coercion below the "armed attack" threshold but military in character and excluding psychological operations, espionage, and economic coercion. Initially, the MCAAC would likely adopt the threshold of "armed attack" in order to address cases most clearly violating international law.

When a state undertakes an operation itself, it is presumed to have "effective control." When the operation is executed via a proxy, the effective control doctrine can apply only when the proxy has "complete dependence" on its state sponsor. The overall control doctrine holds that a state is responsible for a proxy when it contributes to organizing and coordinating the campaign beyond merely providing support. State responsibility below these standards of evidence, including low capacity, negligence, and abetting, overly broaden the initial scope of MCAAC.[35] To address proxies effectively, the MCAAC will likely need to adopt the overall control doctrine. Beyond adoption of careful and manageable legal definitions, MCAAC must conduct investigations at a best practice standard using internationally accepted forensic analysis techniques. MCAAC can gain legitimacy by demonstrating its legal and technical competency and being impartial and transparent.

Given the salience in recent cyber conflicts of nonstate actors, such as patriotic hackers, MCAAC will be most effective in deterrence through attribution if it is able to rule on state responsibility to prevent nonstate actors, whether domestic or foreign, from launching cyber operations from the territory of states they operate from, that reach the threshold of "armed attack." Such rulings will require agreed legal definitions of state due diligence for policing such private actors.

As capabilities for cyber offense proliferate, it becomes ever more urgent to raise the expected level of cyber attribution in order to deter illegal cyber aggression. The prospect of attribution by top tier cyber powers will raise the uncertainty of less powerful actors as to whether they can conduct illegal campaigns without detection and consequences.

To be effective, the MCAAC must employ high security computing and networking technology, narrow compartmentalization, and strong personnel vetting in order to secure the information shared with it by states or other actors. Creative and advanced enterprise security architectures that protect state sources and methods will increase the likelihood of cooperation by states and private sector actors. Indeed, MCAAC should operate as much as possible as a "zero-knowledge"

32 Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law,* vol. 36, 2011.
33 Scott J. Shackelford, "State Responsibility for Cyberattacks: Competing Standards for A Growing Problem," in *Proceedings of the Conference on Cyber Conflict*, C. Czosseck and K. Podins, eds., (Tallinn: CCD COE Publications, 2010).
34 Schmidt, *op. cit.*, pp. 47-52.
35 Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyberattacks," Atlantic Council, 2011.

attribution oracle;[36] it should be opaque as to the provenance of information, where necessary, and yet, implement mechanisms that transparently demonstrate the veracity of claims and facts.

Because fielding a complete MCAAC will require learning and take time, a phased approach could start by experimenting with some joint investigations of major cyber incidents using ad hoc grouping of states and private sector expertise to address specific cases. Even in its early phases, the embedded CBM of joint investigations would help build trust through collaboration and transparency necessary to build over time toward a more comprehensive multilateral attribution regime.

As capabilities for cyber offense proliferate, it becomes ever more urgent to raise the expected level of cyber attribution in order to deter illegal cyber aggression.

Following a major cyber incident, attributing responsibility is important in order to maintain stability, especially if a catalytic actor has sought to exacerbate a crisis between other states. The joint investigation CBM would establish a mechanism to form an ad hoc group of technical experts following a major incident to conduct an international investigation into all evidence to determine which states were responsible. The evidence should include all technical data as well as other pertinent information that aids the investigation in determining responsibility.

Feasibility

The biggest impediment to the establishment of the MCAAC is the desire of states or private actors to protect intelligence sources and methods or indicators[37] used to identify groups responsible for specific cyber campaigns. Without mechanisms to address impediments to sharing relevant attribution information, MCAAC investigators may not be able to follow the chain of evidence in its totality. Divergent political positions by major powers will also skew the process. Naturally, the major cyber powers are unlikely to provide evidence when they are the defendants in a case. Yet, cross-correlation across information from multiple states and private actors may be able to compensate for gaps in the attribution chain.

Integration of evidence from multinational sources may be difficult because the required forensic experts are scarce and states may be unwilling to task them to support the MCAAC. Furthermore, some states may not trust nationals from other countries to access sensitive information. Nonetheless, parallel attribution chains could be developed by different actors, and cross-correlated by MCAAC.

Adjudication is another barrier to acceptance because MCAAC judgments might duplicate some activities of other existing institutions, including the UNSC and the ICJ.

MCAAC will depend for its operation and legitimacy in a large part on the consensus surrounding the legal definitions it employs for the threshold for "armed attack," which defines its scope, and the evidentiary standard for state responsibility, which defines attribution. Indeed, the establishment of MCAAC necessarily must follow development of an international consensus on baselines for these enabling legal definitions.[38] Work toward an MCAAC and its operation once established will drive interpretation and development of international law related to cyber conflict.

Once states are able to come to a general agreement about the need for multilateral attribution to protect countries with lesser cyber capabilities, establishing MCAAC in an initial operational form would take twelve to twenty-four months.

In an architecture for international cyber stability, the crisis management confidence-building measures would contribute to stability, cooperation, and transparency by deterring states from illegal cyber campaigns through higher effective attribution and by enabling states to better manage cyber incidents to avoid uncontrolled escalation into high consequence cyber confrontations or war.

36 Zero-knowledge proofs in cryptography involve proving that an assertion is true without leaking confidential elements of the proof.
37 Indicators of computer network attack are usually often based on tools, techniques, procedures (TTP) employed by specific cyber offense teams.

38 The Group of Experts on cyber threats in the 1st Committee of the United Nations General Assembly could usefully advance workable definitions of "armed attack" and state responsibility necessary to enable the MCAAC.

3. CBMs for Restraint

This section outlines two specific measures that a diverse group of cyber stakeholders can implement in the next several years to increase confidence and stability in cyberspace. These multistakeholder centric CBMs would include applying international law to cyber conflicts by restricting targets for cyberattacks and establishing neutrality statutes for select actors. These CBMs present several different methods to apply international law to cyberspace to increase confidence and limit escalation following cyber incidents.

In addition to the many destabilizers of cyberspace such as deniability of cyber activities and varying concepts of red lines, many states remain at an early stage of maturity with regard to the doctrinal and organizational development of their cyber defense frameworks,[39] adding significantly to possible misperception, misunderstanding, and miscalculation of the risk.

The engagement of various entities in cyberspace, dual use infrastructure, and interconnectivity and interdependencies of the Internet drives the need to shield the entities, persons, and backbone structures of the Internet.

An agreement between states on protected status for critical entities—assets, personnel, and security structures—that keep the Internet running would address the aforementioned challenges.

The goal would be to achieve the acceptance of restrictions of disruptive attacks on specific assets and entities during peacetime, including but not limited to Internet backbone, major Internet Exchange Points (IXPs), finance, aviation, and undersea cables[40] and protected status for critical cyber entities (personnel and organizations) during armed conflict.

Target Selection Restriction

Objective and Scope

International law, both wartime (international humanitarian law, IHL) and peacetime contain red lines of illegality regarding objects of attacks. In the context of an armed conflict, IHL as a matter of law contains limitations on means and methods of warfare, in particular concerning prohibitions regarding attacks on civilian objects.

Peacetime international law contains many limitations relating to targeting certain critical infrastructure.[41] Satellite treaties, treaties covering civilian and military aviation, and International Telecommunications Union (ITU) regulations covering communications include prohibitions on interference or destruction of telecommunication means, which also covers cyber means for such malicious purposes.

There is broad agreement within the international community, restated within the UN Group of Governmental Experts (GGE) that international law applies in cyberspace,[42] but no endeavors have yet been undertaken to provide interpretation of international law in cyber context.

The desired end-state of this CBM would be the acceptance of restrictions, akin to those contained in IHL rules, on disruptive attacks on specific assets and entities during peacetime—including but not limited to Internet backbone, major IXPs, finance, aviation, and undersea cables—that would aim to prevent the "breaking" of the Internet.

Actors

The specific CBM would be a commitment of states to work toward a common understanding of the need to define specific assets and entities that should be granted protective status at all times against disruptive attacks as described above.

Furthermore, commitment of states to develop common understanding of what constitutes specific assets and entities that should be excluded from targeting by malicious cyber activity during peacetime would be a second step in reaching the above-set goal.

Implementation

The measure could be developed through a joint declaration on a common understanding of specific international law regulations that set prohibitions on targeting certain assets by cyber means. An example that could be mirrored for this measure is the Chicago Convention on International Civil Aviation. In the current context, the Convention prohibits any interference with computer networks or systems supporting civil aviation safety.

39 Neil Robinson, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, and Pablo Rodriguez, "Stocktaking Study of Military Cyber Defense Capabilities in the European Union (milCyberCAP)," unclassified summary, RAND Europe, prepared for the European Defense Agency, March 2013.
40 On protection of undersea cables see International Cable Protection Committee, http://www.iscpc.org.

41 Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace.*
42 *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN General Assembly resolution, A/RES/67/27, December 11, 2012; Jen Psaki, "Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues," US Department of State, June 7, 2013, www.state.gov/r/pa/prs/ps/2013/06/210418.htm.

The third leg of the measures contributing to the goal of acceptance of restrictions on specific targets would be joint research on interpretation of international law and its applicability in cyberspace, namely what kind of obligations of states can be derived from the law in terms of cybersecurity.

This measure could be implemented both unilaterally and multilaterally.

On a state-to-state level, the state parties would establish an inter-agency working group on ministerial level to develop a common understanding of the specific assets, informed by and with contributions from relevant national and international nongovernmental organizations.

The group would convene for the first time six months after the codification of the CBM and would continue its work through regular meetings at intervals to be agreed.

Because of its standing in the area of codification and progressive development of international law, the UN would be a suitable forum to feed discussion on development of norms in this area. Diversity of approaches toward international law could, however, render UN process in this area ineffective.

The OSCE, on the other hand, has experience and success in formulating CBMs and reaching agreements between states, and would thus be the most suitable forum for the aforementioned measures. Although, the organization is more focused on discussion and collaboration, the CBMs developed within the OSCE are perceived, at least within the organization, as an essential part of the norm-building process, even though political in nature.

Unilateral declarations and statements, in which state representatives declare Internet backbone, major IXPs, finance, aviation, and undersea cables off limits for cyberattacks can serve as a transparency measure and contribute to the overall stability of the Internet.

A bottom-up approach, based on the track two agreements between organizations such as think tanks or the ICANN, would be a productive start toward work on state-to-state level.

Feasibility

The biggest impediment for state agreement on such norms are the difficulties in clearly delineating the definition of armed attack in cyberspace and legal distinctions between state or armed conflict and jus ad bellum, serves as potential blockers for development of this norm.

One practical and relatively timely remedy that does not involve the controversial question of applicability of international law in cyberspace would be political declarations of states, which are a powerful tool of international relations. Importantly, they are also significant for the progressive development of international law.[43]

Neutrality Status

Objective and Scope

International humanitarian law (IHL) protects a wide range of persons and objects during armed conflict, namely civilians not directly participating in hostilities, medical and religious personnel, and civilian objectives. Based on the protection afforded by the IHL, the aforementioned persons and structures cannot be the object of an attack during an armed conflict.

Neutrality, in international law describes the formal position taken by a state that is not participating in an armed conflict or that does not want to become involved. This status entails specific rights and duties. On the one hand, the neutral state has the right to stand apart from and not be adversely affected by the conflict. On the other hand, it has a duty of nonparticipation and impartiality.[44]

Drawing upon these two concepts from international law, the desired end state of this CBM would be a protected status for critical cyber entities, such as personnel and organizations, during armed conflict.

This measure could achieve neutrality status (legal or political) for critical cyber havens, whether organizations or cybersecurity personnel and would benefit these entities during wartime.

Private entities, due to their deep involvement and tasks they perform in cyberspace, exacerbated by the dual use of cyber infrastructure, can face entanglement in interstate conflicts. Because of the crucial role of these entities in keeping the Internet up and functioning, they should be afforded protected status.

Actors

This specific CBM would entail state parties' commitment to achieve common understanding of the need to confer protected status to critical cyber entities during armed conflict, and to join efforts toward establishing such protected status on a global level.

The second leg of the measure is state parties' commitment to develop common understanding of what constitutes critical cyber infrastructure both in terms of technical infrastructure, entities maintaining

43 Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace.*
44 International Committee of the Red Cross, Unit for Relations with Armed and Security Forces, "Law of Armed Conflict: Neutrality," June 2002, www.icrc.org/eng/assets/files/other/law8_final.pdf.

critical services, and their personnel, between state parties to the agreement of the CBMs and at the global level.

Implementation

This measure could be implemented both unilaterally and multilaterally.

On a state-to-state level, an inter-agency working group on ministerial level to develop a common understanding of the need to confer protected status to critical cyber entities, informed by and with contributions from relevant national and international nongovernmental organizations, would be established. The group would convene for the first time six months after the conclusion of the CBMs and would continue its work on a basis of regular meetings at intervals to be agreed.

Because of its standing in the area of codification and progressive development of international law, the UN would be a suitable forum to feed discussion on development of norms in this area. Diversity of approaches toward international law, however, may render UN process in this area ineffective.

OSCE, on the other hand, has experience and success in formulating CBMs and reaching agreements between states, and would thus be the most suitable fora for the aforementioned measures. Additionally, the organization focuses more on the process of discussion and collaboration, rather than precise norm, which in itself contributes to stability and transparency between states.

Unilaterally, state representatives can declare that they consider critical cyber infrastructure—both in terms of technical infrastructure, entities maintaining critical services, and their personnel off limits—for cyberattacks can serve as transparency measure and contribute to the overall stability of the Internet.

A bottom-up approach, based on the track two agreements between organizations such as think tanks or the ICANN, would achieve the goal of stability and would be a productive start toward work on state-to-state level.

Additionally, cyberspace militarization, in particular, drives the need to shield the entities and persons who run the Internet from cyber incidents in peacetime. Thus, a development of similar measure to that for armed conflict situations could be considered for peacetime.

Feasibility

The blocker that could frustrate progress in development of this norm is the unsettled definition of armed attack in the cyber domain and varying interpretations of international law applicable in cyberspace. To overcome this possible blocker, states should focus on referent objects, without the need to mention or agree on what constitutes an attack. To avoid the problem of defining when we are in peace time and wartime, countries could agree on a universal protection status that applies regardless of whether we are in an armed conflict or not.

Unilaterally, state representatives can declare that they consider critical cyber infrastructure off limits for cyber attacks.

4. CBMs for Engagement

This section outlines two specific measures that a diverse group of stakeholders can implement in the next several years to increase confidence in cyberspace. These multistakeholder centric CBMs would include engaging neutral activists in cyberspace to support other neutral actors and leveraging existing technical regimes to establish international norms.

These two CBMs present several methods to engage nongovernmental organizations to increase stability in cyberspace and work to establish norms and standards for cyber actions.

Leveraging Technical Regimes for International Norms

Objective and Scope

Existing technical regimes can provide a practical side channel for communicating international cyber norms. Technical regimes have an existing working process to establish international technical standards that can serve as a side channel for policy communication on international norms. Requests for Comments (RFCs) by the Internet Engineering Task Force (IETF) are one example of a technical side channel for international norms.

Leveraging technical regimes to establish international norms would combine the expertise of both regime types to enable dialogue about appropriate norms.

The specific CBM would be a commitment of states to work toward a common understanding of the need to leverage existing technical regimes into new processes. After the initial agreement of states, this norm would be developed in a bottom up process.

Actors

The CBM will primarily focus on the technical side but will bring the technology community in conversation with policymakers. Specifically, existing technical organizations—IETF, the World Wide Web Consortium (W3C), the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Society (ISOC), and others—will work with multistakeholder-minded governments to assist in the establishment of international norms. Collaboration between both regime types would leverage the technical expertise of the technical organizations with the policy expertise of the policy organizations and governments to create a side channel for communication on international norms.

Implementation

This CBM would not seek to establish specific norms but would serve as a process for agreeing to and codifying existing international norms. The CBM would provide a communication channel that would take advantage of the existing channels established by the technical regimes and use them to establish appropriate norms and policies.

There are several possible norms amenable to this regime. It could provide assistance to organizations under attack through technical support, including filtering attack traffic. It could also provide global coordination to respond to major Internet incidents and shocks by providing a communication channel for international technical and political regimes. The regime could also establish a code of conduct for any organization owing an Autonomous System solidifying rules for how to establish such a system and how they are to be employed. Finally, the regime could facilitate policing existing best community practices.

Feasibility

The regime would implement control solutions important to governments through existing technocratic paths. This process should be relatively inexpensive, as it does not seek to establish new channels or organizations for communication, but instead seeks to improve upon existing processes. The use of existing channels and organizations should also take minimal political effort to establish and may be easy to adopt if the existing technical regimes are willing to fill this new role.

Some possible hindrances to establishing this regime and new CBM are the willingness of governments and the existing technical community to accept the new role. Such a CBM is different from what governments typically consider an international norm or CBM and as a result they may not be comfortable with its establishment. This CBM also requires the technical community to take on increased responsibility beyond their traditional technical role, the community may as a result be reluctant to take on the increased responsibility outside of its traditional role. The reluctance of governments and the technical community may delay the adoption of such a CBM and could require several years before it is fully operational.

In the trinity of the goals of CBMs—transparency, stability, cooperation, the measures described in this report—contribute foremost to collaboration and stability by engaging state and nonstate actors in way that leverages their expertise for the stability of cyberspace and that utilizes existing technical regimes in a new way.

Neutral Activist Entanglement and Support CBM

Objective and Scope

The basic idea of this norm is to build trust and confidence by encouraging security researchers to collaborate on important issues across borders. A pertinent example of such an existing organization is I Am the Cavalry, which describes itself as a "global grassroots organization that is focused on issues where computer security intersects public safety and human life."[45]

Access to cyberspace, unlike traditional domains, is not limited to states and well-funded actors but all levels of actors are able to have a significant impact in cyberspace. Unaffiliated security researchers and other individuals are some of the most significant and thereby some of the most dangerous and destabilizing actors.

Access to cyberspace, unlike traditional domains, is not limited to states and well-funded actors but all levels of actors are able to have a significant impact in cyberspace.

Currently, there is little incentive or structure for these actors to apply their skills in a manner that supports the common good. Leveraging these actors' skills to protect and support vital elements of cyberspace would serve the dual purpose of removing their destabilizing effects on the environment and applying their skills in a productive manner.

Furthermore, states have been unable or unwilling to take necessary steps to protect cyberspace and provide support for compromised regimes that rely on the Internet.

Providing a platform for nonaffiliated actors to make a positive impact in cyberspace would represent concrete step toward protecting these critical elements of the cyber infrastructure that states have failed to secure. Creating such a platform would also allow these actors to provide logistic support and engagement in cyberspace to protect critical elements of the cyber infrastructure.

Neutral Activist Entanglement and Support would take the form of an internationally sponsored platform that encourages the development, success, and collaboration of independent community and civil society organizations. Members' incentives to participate would include gaining access to resources that they would not be able to access independently and improving their international stature.

The specific CBM would be a commitment of states to work toward a common understanding of the need to provide support for nonaffiliated actors. This would be followed by establishment, on a state-to-state level, an inter-agency working group that would develop the details of the financial and logistical support required for these groups. After this initial state involvement, the measure would be a bottom up process.

In addition to the resources and freedom of action for actors, the platform would provide a legitimate outlet for many unaffiliated cyber actors under existing international cooperation frameworks and allow them access and influence within formal international policy channels.

This would elevate their level of participation and provide a voice for cyber stability at the international level.

Actors

The targeted organizations would optimally comprise of security researchers and other independent actors whose productive and stabilizing interests have been supplanted by the rise of commercial interests.

Organizations with local, national, and international cyber capabilities that are primarily focused on using these capabilities in support of common interest security concerns, including health and safety, would be included.

Implementation

Such a platform for use by targeted organizations and other unaffiliated actors would help increase confidence and stability by

- engaging potentially destabilizing independent actors in predictable, benign activities;
- increasing resilience of the Internet by leveraging currently destabilizing independent actors talents;

45 I Am the Cavalry, www.iamthecavalry.org.

- entangling interests of a diverse set of international actors that are beyond the reach and influence of traditional institutions;
- assuring the existence and engagement of a community with individually motivated interests in maintaining the overall stability of cyberspace;
- providing continually available and easily accessible dynamic recovery capabilities; and
- creating a substantial but ungoverned buffer against inadvertent escalation.

This platform should be developed by a collaboration of existing organizations that, collectively, have the capacity to offer opportunities to those security researchers and other independent actors that do not have access to similar platforms on their own.

The organizing regime for this platform would provide specific criteria for targeting individuals and organizations for participation in the platform. It would also establish "rules of behavior" that all participating members must abide by in order to continue participating and maintain political protection for their activities. These rules would be established in consultation with relevant states and international organizations based on new agreement between the relevant parties for what operationally and technologically constitutes politically protected activities.

The regime would also provide operational mechanisms for platform-subscribed organizations to participate in international legal and policy dialogue. This dialogue would be supplemented, where practical, by providing voting rights in international organizations and decision-making bodies.

It would establish guidelines for state interaction with platform subscribed organizations in order for those organizations to maintain an appropriate level of independence. The regime should also provide messaging and marketing support and consultation for individual states on how to identify, create, and engage applicable organizations.

Feasibility

In order to implement this CBM, there are two primary conditions that must be met.

First, in order to engage actors in the platform there needs to be a sufficient number of organizations that fit these criteria and are willing to engage. While there is at least one organization that fits these criteria, I Am the Cavalry in the United States, its willingness to participate is undetermined, and it is unknown if other organizations exist that are appropriate for engagement. The success of the CBM does not depend, however, on retargeting these originations missions or operations. As long as the goals of the organizations and the regime remain aligned, the targeted organizations' cost of participation will remain low. Furthermore, the benefits of participation may encourage the formation of new organizations that align with the regime's objectives.

The second condition is the willingness of states and associated organizations to provide the necessary recognitions and support to platform subscribed organizations. States should consider protection to the platform in order for it to maintain legitimacy and provide incentive for existing organizations and individuals to subscribe to the platform over other existing options that are less desirable and destabilizing for the international community. The value of the CBM's process and engagement will outweigh any specific activity set and therefore it is likely that a reasonable and accepted set of practices, policies, and recognition can be identified and created.

In the trinity of the goals of CBMs—transparency, stability, cooperation—the engagement measures would contribute foremost to the stability of interstate cyber relations by reinforcing the collaboration between nonstate actors globally in assuring that minor cyber incident do not escalate and states share information in a transparent manner.

Cyber conflict stretches the traditional notion of confidence-building measures. The actor set expands from states to include the private sector, which operates critical infrastructures like the financial system, telecommunications, power grids, and energy infrastructure.

Conclusion

Confidence-building measures are a longstanding construct for politico-military risk reduction among states.[46] They assume that hostilities can occur through accident, misperception, or miscalculation. In cyberspace, the assumption is that the complexity of the cyber dimension offers many opportunities for mistakes, misperceptions, and miscalculations, and so CBMs can play an important role in risk reduction.

Cyber conflict stretches the traditional notion of confidence-building measures because the actor set expands from states to include the private sector that operates critical infrastructures like the financial system, telecommunications, power grids, and energy infrastructures. Whereas CBMs have traditionally been used to reduce risk of war, most malicious cyber activity takes place well below thresholds of "armed conflict," as defined under international law.[47]

Additionally, sustained patterns of aggressive cyber activity at lower intensity, including preparation of the battlefield, can cumulate to national security threats.[48]

46 For an overview of confidence-building measures, see Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace*.
47 For a major discussion on the applicability of international law to cyber conflict, see Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).
48 An example such cumulative impact of aggressive cyber operations may be the economic disruption caused by large scale state-sponsored industrial espionage for commercial gain. *The IP Commission Report, Commission on the Theft of Intellectual Property* (Washington, DC: National Bureau of Asian Research, May 2013).

To face these challenges in cyberspace, the existing confidence-building regimes and mechanisms have to be supplemented by new approaches.

The development of these measures described in this report is contingent on a new approach to CBMs, one that recognizes that bottom-up approach to norms of behavior in cyberspace, aided by multi and bi-lateral state-to-state actions and support, are the most conductive to security, stability, and collaboration in cyberspace. Some of the proposed measures build on existing constructs in international relations, such as best community practices (BCPs) in cyberspace, and propose new ways of implementing them. Others, such as Multilateral Cyber Attribution and Adjudication Council (MCAAC) suggest new international mechanisms for arriving at a consensus in attributing malicious activities in cyberspace. The four types of proposed CBMs and the individual measures are designed to provide a diverse set of multistakeholder ways to increase stability and build confidence in cyberspace without extensive legal or political action by states. These measures can all be implemented independently and each has varying feasibility in the current international and political climate.

Atlantic Council Board of Directors

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 778-4952, www.AtlanticCouncil.org