Confidence-Building Measures

The Future of the Global Information Infrastructure

Anatoly Streltsov

Creating confidence-building measures in the information sphere has become a major foreign policy priority for many states.¹ Confidence-building measures and other collaborative efforts to counter military, terrorist, or criminal threats create conditions for the maintenance of international peace and security in the information sphere. Confidence-building measures in the information sphere are similar to confidence-building measures between militaries in that they are a set of measures that facilitate information sharing between states regarding their information and communication technologies and strategies.² The measures are created to neutralize the cyber threats of opposing states in peacetime and wartime, to prevent and resolve crises in the area of information infrastructure, to combat cybercrime and information terrorism, and to promote states’ national cultural values and political preferences in foreign countries.³

As such, confidence-building measures are used as instruments in maintaining international peace and security and provide an environment of mutual understanding between nations. This environment reduces the risk of a surprise attack on key national information infrastructure facilities or a politically-motivated, violent conflict triggered by

Anatoly Streltsov
is the Vice-Director of Lomonosov Moscow State University’s Information Security Institute. He has worked as a Research Physicist in the Naval Research Laboratory and as a Research Associate Professor at Dartmouth College. His research in physics and mathematics has been sponsored by NASA, ONR, Air Force and DARPA.
"information weapons." In this paper, ‘information weaponry’ is defined as special information technologies and communications technologies; this includes attempts to violate computer security by using a piggyback entry, tailgates, and aborted connections. Confidence is the only tool that can be used in international cooperation on cyber. Confidence is the first step in developing proposals for the formation of responsible state behavior in the information sphere.

Information security has been discussed at the UN General Assembly, at the UN Group of Governmental Experts, and at international conferences and seminars over the last decade. These discussions are important in that they have allowed the international community to develop the political capital required to reduce the danger posed by the malicious use of information and communications technologies, criminal organizations, and individuals. Meetings held between the United States and Russia in 2010 and 2011 on global information security demonstrate this potential. What emerged from these meetings is a joint U.S.-Russia statement on measures to enhance confidence in cyberspace. The statement recognizes that the relationship between the two countries on cyberspace security has advanced to a new level, making it possible to build confidence and ensure transparency. In addition to these efforts, the international community has already developed and implemented some confidence-building measures, examples include the exchange of information on cybersecurity between the members of NATO. Similar work in the field of information security has been carried out within the framework of the Union State of Belarus and Russia, as well as by the members of Collective Security Treaty Organization (CSTO).

However, because confidence-building measures can mitigate threats to states’ national interests, international peace, and security, much remains to be accomplished in this area.

This first section of this paper explores four threats of information infrastructure and how confidence-building measures can be used to eliminate these threats. The second section of the paper explores three potential scenarios that can result from different levels of confidence-building measures.

**Threats to global information infrastructure and confidence-building measures.** The report that followed session 65 of the UN General Assembly outlined the following four threats: (1) use of information and communications technologies as warfare and intelligence tools towards political ends; (2) use of information and communications technologies to plan and organize terrorist activities; (3) use of information and communications technologies as a crime tool in the information sphere; and (4) use of the global information infrastructure for subversive activities, including activities carried out by individuals, groups, and organizations, to perform intermediary functions in organized subversive activities on behalf of other persons. This section of the paper will discuss each of these four threats and explain how confidence-building measures can mitigate or overcome these threats.
The threats listed by the UN impact most significantly the development of states’ foreign policy concerns relating to national and international information security. The first threat of information and communications technologies used as tools of warfare and intelligence for political ends raises three major concerns. The first concern is that if information and communications technologies are used as means of warfare for political purposes there is the possibility to disrupt the stable operation of the Internet, which is the foundation of the global information infrastructure. This is especially troublesome since many nations are working on expanding the global information infrastructure in an effort to meet commitments that the World Summit on the Information Society (WSIS) established in 2003 and 2005. The objective of the WSIS is to develop e-commerce, enable government authorities to provide information services to their citizens, enhance transparency of government control, expand international cultural exchange, develop distance-learning systems, and improve healthcare. Thus, destabilizing the operation of the global information infrastructure can produce grave implications; determining quality standards for those services; and internationalizing the process of taking and implementing decisions to control the stable operation of the network in emergencies caused by political and terrorist factors.

A second concern is the ability to include latent malicious functions in these technologies. This is especially important in light of research and efforts by states to create 'information weapons.' This threat increases with the resulting temptation to integrate confidence-building measures should be built in such a way as to involve interested nations to perform certain Internet control functions that would remove the concern of technologies being used as warfare. However, not all Internet control functions are equally important in sustaining the stable operation of the global information infrastructure.

To overcome this threat confidence-building measures should be built in such a way as to involve interested nations to perform certain Internet control functions that would remove the concern of technologies being used as warfare. However, not all Internet control functions are equally important in sustaining the stable operation of the global information infrastructure. If we assume that the main network operation controls are handled by Internet providers then, regarding the implementation of confidence-building measures, it would be possible to start discussing the following issues: developing the international regulatory environment of Internet services; determining quality standards for those services; and internationalizing the process of taking and implementing decisions to control the stable operation of the network in emergencies caused by political and terrorist factors. Because non-government structures perform functions to control this network, it is important to ensure coordinated operation of these non-government actors and newly established government authorities.
such ‘weapons’ into information and communications technology products available in the market. This potential substantially heightens the risk of destabilizing the operation and security of key national information infrastructure facilities and creating situations with the potential for international conflicts.

This concern can be decreased if confidence-building measures focus on setting up forums to establish the following measures: setting special safety standards for information and communications technology products, introducing a system of voluntary certification to meet the above standards, and establishing an international judicial body to review claims of certified-product non-compliance with requirements and enforce liability for offenders.

The third concern that this threat raises is the risk of an ‘information arms’ race and the use of information weapons. A growing number of states utilize information weapons as support for or in lieu of traditional kinetic weapons. Stuxnet, Flame, and other viruses demonstrate the destructive capabilities and the dangerous implications of malicious software. The trends in upgrading ‘information weapon’ destructive capabilities show the same pattern.

In these conditions the concern could be eliminated by adopting international legal instruments. This would involve developing norms of international humanitarian law, international security law, and laws of war as they apply to the use of the ‘information weapon’ in interstate conflicts. An international hotline that authorized representatives of states could call to discuss suspicions and misunderstandings, a communications channel between members of the UN Security Council, and an intergovernmental agency tasked with conducting joint investigations on the employment of information and communications technologies should all be established. This cooperative effort would disrupt the threat posed by key national information infrastructure facilities to other national information infrastructures.

The second threat to international information security, as outlined above, is that information and communications technologies can be used to plan and organize terrorist activities. Terrorist organizations and individual terrorists can access prototyped ‘information weapons’ and the methods that can be used to employ such weapons for political purposes. Information and communication technologies can be used to facilitate the preparation of terrorist acts and harmonization of terrorist groups’ actions, as demonstrated by the terrorist attacks in the United States on 9/11 and in Mumbai, India, on 26 November 2008. On the one
hand, the international community is working to impede terrorists from using 'traditional' means of committing acts of terror and to interdict access to nuclear weapons. On the other hand, nations are working to upgrade their national information infrastructure and technological capabilities. Using an 'information weapon' in an attack or to coordinate an attack are tactics garnering increased attention from terrorists. Although to date there is no case of successfully employing information and communications technologies to carry out acts of terror (9/11 and the Mumbai attacks information and communication technologies were used to prepare the terrorist attacks, not directly carry them out), the likelihood of such an event is rising.

In this case, as well, confidence-building measures can eliminate the threat. They could include, for example, information sharing regarding the aspirations of terrorist organizations and individual terrorists to gain access to prototyped information weapons and methods of employing such weapons. Sharing this information would enhance national efforts to prevent terrorist organizations from accessing information about the research and development of information weapons, detect and suppress the activities of terrorist organizations, and reduce the risk of confusion in the use of information weapons by nation states.

The third threat to international information security, as outlined by the UN General Assembly, is that information and communications technologies can be used to commit "information crimes." In spite of considerable efforts by law enforcement services, thus far there is nothing that can be done to alleviate information criminality. This is partly due to the trans-border nature of most information crimes and the nascent state of international cooperation in crime investigations. The Budapest Convention on Cybercrime was adopted in 2001 with the purpose of addressing information criminality but the situation has not changed. The Budapest Convention has actually generated new concerns about the potential use by foreign law enforcement agencies to access information infrastructure facilities for illegal activities. For example, information access could be used to review personal details of citizens and industrial and military secrets, and to install 'information weapon' components at national information infrastructure facilities.

To overcome this threat, confidence-building measures could include the adoption of an international treaty to combat cybercrime which would address mutually beneficial mechanisms for fighting information crime and could draw from existing international treaties regulating this area. Such a treaty would allow government authorities and international organizations, such as INTERPOL, to fight computer crime.

The fourth threat to international peace and security is that the global information infrastructure can be used for subversive activities. This threat raises the concern that some states could use information agencies, social networks, and other information and communications technologies to undermine the stability of foreign states, to support decisions to use military force, or to force independent
nations to change their policies. Foreign states that publish information on biological and chemical weapon systems, violations of human rights to freedom of speech and expression, or inadequate attention by states to existing humanitarian problems could spark the subversive activities listed above. In this case, exchanging information can be used to manipulate public opinion by other states and international organizations.

**Scenarios.** The importance of countering these four threats is evidenced by the Intergovernmental Agreement on Information Security signed by the Member States of the Shanghai Organization in July 2009. One goal of this multinational organization is to build information security. To achieve this, the Member States must establish confidence-building measures. Trust between states is crucial for international cooperation, especially to counter threats to international information security. The level of confidence-building measures that states employ and how they are implemented will impact the development of information infrastructure. This section of the paper considers three scenarios that could result from different levels of confidence-building measures. The future of the global information infrastructure depends on many factors, but one of the most important is how confident states are that investing in the development of the global information infrastructure will not be used by foreign states to damage national economies, destabilize public administrations, or undermine human rights and sovereignty in the information sphere.

**Scenario 1:** In this scenario the maximum level of security is achieved due to successful implementation of confidence-building measures: the global information infrastructure continues to grow and citizens, businesses, and government authorities maintain a high level of confidence in the implemented infrastructure. Cooperation among law enforcement agencies is efficient, thus reducing the risk of information crime and information terrorism. The use of information and communications technologies in business processes and government authorities increases; businesses turn to these technologies as the capitalization of companies involved in the creation and development of these technologies increases. Furthermore, governments use these technologies to provide services to communities. This situation helps achieve a sufficient degree of protection for the national interests of Member States of the international community, related to information and communications technologies, from malicious activities by foreign states. Circumstances
improve the transparency of government activities and, as a result, efficiency of control over government activities by the society and interested non-government organizations. Democratic procedures of society’s participation in public administration develop. The level of industrial and military espionage raises no concern with states.

Scenario 2: In a less favorable but more realistic scenario, the global information infrastructure develops with limited and inadequate confidence-building measures. States are concerned about national and international information security. The global information infrastructure positively affects the development of the global information economy but less so than in the first scenario. Information risks present in businesses rise.

The use of the global information infrastructure to enhance the economic potential of states is confined by significant political risks. The use of foreign information and communications products in setting up key national information infrastructure assets, information, and communications products is restricted. International cooperation in information and communications technologies is suppressed by states and regional organizations. There remains the risk of encroaching on the national interests of Member States of the international community.

However, the level of confidence by citizens, businesses, and states in the infrastructure remains sufficiently high to support its development. Countermeasures provided by law enforcement agencies to combat information crime remains inefficient and criminal activities continue to increase. Spontaneous disruption of operations at key national information infrastructure facilities caused by both terrorist organizations and security agencies of foreign states becomes more frequent. Interventions are discussed more often at UN Security Council meetings and states budget more money for countermeasures in the global information infrastructure.

There is an ongoing fierce information fight in the mass media which is attributed to attempts made by foreign states and their non-government affiliates to interfere with the internal affairs of other states. At times, low intensity armed conflicts erupt out of deep political controversies over the sociopolitical implications of the disrupted operation of key information infrastructure facilities. States and their regional authorities undertake some measures to single out the national information infrastructure into a relatively independent global information infrastructure segment. States continue to exercise certain restrictions on human rights to freedom of information exchange and expression. State security services continue with their active efforts to gain illegal access to industrial and state secrets.

Scenario 3: In the worst case scenario the global information infrastructure develops without any confidence-building measures. States and their regional authorities isolate information infrastructures into independent information and communications networks. As a result, the global economy degrades and stagnates, isolating national economies, due to the deteriorated efficiency of international cooperation in industry and trade. Risks relating to the use of information and communications
technologies are high, which undermines the development of an information economy.

Citizens, businesses, and government authorities have almost no confidence in the global information infrastructure. There is no interface between states in computer crime - information criminals and terrorist organizations use information and communications technologies for their own purposes. The level of social risk is high.

Information fighting in information infrastructure between opposing states become fiercer. This fighting disrupts the operational capabilities of national communications systems and satellite constellations. Armed conflicts are common among states and can potentially trigger a world war. Enforcing human rights and freedoms globally is no longer a priority to nations that are more concerned with countering military threats. Spontaneous disruption of capabilities of key national information infrastructure facilities committed by terrorist organizations and foreign states are common, which contributes to the formation of a hostile multipolar world. States actively integrate information weapon components into information and communications systems of foreign states, thus raising suspicions between states. Information fighting in the mass media is attributed to attempts made by states and their non-government affiliates to interfere with internal affairs of other states.

Conclusion. International peace and security in the information sphere is necessary to realize the full potential of information and communication technologies, while simultaneously respecting the rights and freedoms. Achieving international peace and security is possible only through international cooperation and confidence-building measures in the field of information security, which will create a sense of trust among states. The substance and scope of the confidence-building measures implemented by states will shape the future global information infrastructure. This paper has discussed the four threats to the global information infrastructure outlined by the UN General Assembly and how confidence-building measures can be used to overcome those threats. The second section of the paper examined three potential scenarios that could result from different levels of confidence-building measures implemented into the international system. The most favorable scenario of the future global information infrastructure is feasible if confidence-building measures are developed to help states ensure human rights and freedoms, provide free and independent development of national communities, improve the well-being of citizens, and preserve its cultural integrity and safety.
1 The information field represents the totality of public relations-related information and information infrastructure.


4 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN A/65/201 (30 July 2010).

5 Ibid.


7 Report of the Working Group on Internet Governance, 05.64122 (June 2005).

8 Recall ‘information weapons’ are special information technologies and communication technologies, including technologies used to violate computer security.

9 Agreement Between the Members of Shanghai Cooperation Organization in the Field of Information Security, 15.06.0001 (2009).

10 The idea for these three scenarios is based on Jason Healey’s predictions for five future possibilities of cyber conflict. Jason Healey, “The Five Futures of Cyber Conflict and Cooperation,” Georgetown Journal of International Affairs Special Issue: Cybersecurity, (2011).
Raytheon delivers the talent, technology and partnership organizations need to ensure continued operations in the face of persistent threats. Our layered Cyber Resiliency strategy leverages over three decades of expertise to help you anticipate, withstand and recover from cyber attack — and to evolve as new threats emerge. Raytheon. Be ready. Be resilient.