International Cybersecurity Information Sharing Agreements

Phase I Study Report | October 2017

Theresa Hitchens & Nilsu Goren

SCHOOL OF PUBLIC POLICY
CENTER FOR INTERNATIONAL & SECURITY STUDIES AT MARYLAND

Acknowledgements: This report was prepared as part of CISSM's Multi-stakeholder Approach to Cybersecurity Risk Management Project, with support from the Laboratory for Telecommunications Sciences. The authors would like to thank graduate assistants Jeremy Hiken and Renuka Pai for their work in support of this project.

Introduction

Cybersecurity transcends national boundaries in many ways: The internet's technical infrastructure is global in scope; threat actors based in one country can disguise their identities by taking control of computers in other countries; global businesses sell software, hardware, and security services that may introduce or combat vulnerabilities; and the consequences from a disruptive attack can spread far beyond the initial victim. Even the most cyber-savvy country cannot protect itself completely unless it wants to disconnect from the global internet and strictly limit who can use information technology and for what purposes inside its own borders. And this course of action is infeasible because it would result in dire consequences for the national economy, military, and all other systems that depend on advanced information technology. International cooperation to improve cybersecurity is a much more realistic and viable path. Information sharing is the most commonly promoted type of international cooperation, but very little is known about what type of cybersecurity information is currently being shared with whom, for what purposes, and under what conditions.

As a first step towards answering this larger question, the International Cybersecurity Information Sharing Project undertook to survey, catalog, and analyze publicly available government-to-government cybersecurity-related sharing agreements to determine what types of information various governments have committed to share, and to identify gaps in information sharing. The ultimate aim of the larger project is to assess how multilateral cybersecurity sharing practices can be encouraged and improved in order to strengthen global cybersecurity.

The project team started from the assumption that formal cyber sharing agreements and memoranda of understanding (MoU) are an important part of the foundation for the development of norms on cyber cooperation. Over the past several years, various international fora have reiterated that sharing information about cyber threats and vulnerabilities, national approaches to cyber protection, best practices, incidents of concern, and response mechanisms could increase mutual cybersecurity while reducing risks of misunderstandings and conflict.

Different types of information sharing can be used to improve cybersecurity in various ways. By sharing threat perceptions and national policies, states can better understand each other's concerns and priorities. By conducting multilateral exercises and sharing best practices for protection of networks, critical infrastructure, and software/hardware, states can help each other ensure safe data transfer across borders. Cooperation to build capacity in states with weaker infrastructure for managing the use of information and communications technologies (ICTs) can help in identifying threats and responding to crises.

This research found that cybersecurity information agreements are more numerous, but less specific than anticipated. The project documented and analyzed 196 agreements involving 116 different countries and 2,349 signatures. Extensive signature of agreements and associated commentary shows widespread accord on the principle that information sharing is necessary. However, it is unclear how much and what type of information sharing occurs in practice. Few agreement texts are public, and those that are often use vague language. And, despite the potential benefits of sharing more cyber-security information, many disincentives and logistical

barriers remain. This project collected as much information as possible, not only about what states have agreed to do, but also what they actually do, and why they make those choices.

After a brief summary of the approach taken and some limitations encountered, the study provides summary statistics about international cyber information sharing agreements. It then looks in more detail at sharing agreements and behaviors by some of the most active and/or important countries in regional organizations, and in multilateral fora that have focused on this topic. A summary of key findings, conclusions, and next steps is followed by annexes with more methodological information and texts for some of the most important agreements.

Approach

Cybersecurity is defined broadly as: measures taken to protect a computer or computer system against unauthorized access or attack. Numerous actors besides states are engaged in cybersecurity cooperation, including private companies, universities, and non-governmental organizations. Moreover, government-to-government cooperation usually is not focused on high-level legal arrangements. Instead, it is spread out to include governmental agency-to-agency activity, government-sponsored fora for exchange of information, non-governmental organization meetings, and membership organization meetings such as at regional forums. Thus, the scope of the research was widened to include these sorts of formal and informal activities, as long as they were at least somewhat institutionalized rather than purely ad hoc, and involved sharing information about cybersecurity for primarily non-commercial purposes. Given the differences among countries in cyber-related terminology, agreements about information and communications technology (ICT) that fit these criteria were also included even though they did not use the term "cybersecurity."

Rather than attempt a world-wide survey, this initial project focused on members of major regional organizations that have shown particular interest in cybersecurity: the Organization for Security and Cooperation in Europe (OSCE), NATO, the European Union (EU), the Association of Southeast Asian States (ASEAN), and the Shanghai Cooperation Organization (SCO). This means that African, Latin American, and Middle Eastern countries are under-represented in the current survey. This decision enabled us to spend available time and resources to develop a more complete picture of cooperation involving the most active countries.

Data collection was built on the International Telecommunication Union's (ITU) cybersecurity maturity reports on 195 countries, and on the 2013 literature survey "The Cyber Index: International Trends and Realities."[1] To find additional multilateral, regional, and bilateral agreements, CISSM researchers scoured English-language news media, trade publications, and other documents. Additional information was collected about the most important agreements by contacting government officials and cybersecurity experts. Using only English-language open sources of information may have reduced the relative number of agreements researchers found involving non-English speaking countries that do not get extensive attention from English-language media sources.

[1] Theresa Hitchens, ed., "The Cyber Index: International Trends and Realities," United Nations Institute for Disarmament Research, 2013, http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

The third limitation of the survey was that it could only capture what was available in the public domain. Researchers found that few agreement texts have been made public in full, beyond media statements indicating the intent to cooperate or that a memorandum of understanding (MoU) on cybersecurity was recently signed. Further, those agreements that are in the public domain are often vague, making it difficult to assess the actual impact or implementation of the agreements. Even more difficulty was encountered in documenting incidents where such agreements have been invoked or utilized, perhaps due to reluctance on the part of governments to publicly discuss breaches of information or networks. Understandably, details of technical information sharing agreements between Computer Emergency Readiness Teams (CERT) were also not publicized. However, patterns of cooperation are visible and can be used to elucidate some questions about how states interact with regards to cybersecurity.

Even with limits imposed by geographical scope, language constraints, and the classified or sensitive nature of the cybersecurity sphere, researchers found a surprisingly large number of agreements, often involving more than two signatories. At a macro-level, the research documented 196 agreements involving 116 countries. In total, these agreements involve 2,349 signatures when broken down by type.

The agreements were categorized into the following types:

Training – Agreements that involve training of personnel, either mutual or in one direction.

Research – Agreements that involve working together on research about risks, threats, methodologies for detection of intrusions, etc.

Policy – General cooperation agreements that include exchanges on cybersecurity policies, laws, identification of critical infrastructure, at a government-to-government level.

Information Sharing – The most general of the agreement types, ranging from high-level political agreements to agency-to agency agreements to share a broad, or vague, scope of information regarding cybersecurity.

Military – Agreements that specify cooperation between ministries of defense, and/or military forces.

Cyber Operations – Agreements that involve countries working together to thwart cybersecurity breaches, build up cyber defenses, technical cooperation on protection, detection and incident response, and CERT-to-CERT agreements.

Cyber Exercises – Agreements that involve conduct of joint exercises and simulations practicing cyber defense or response operations.

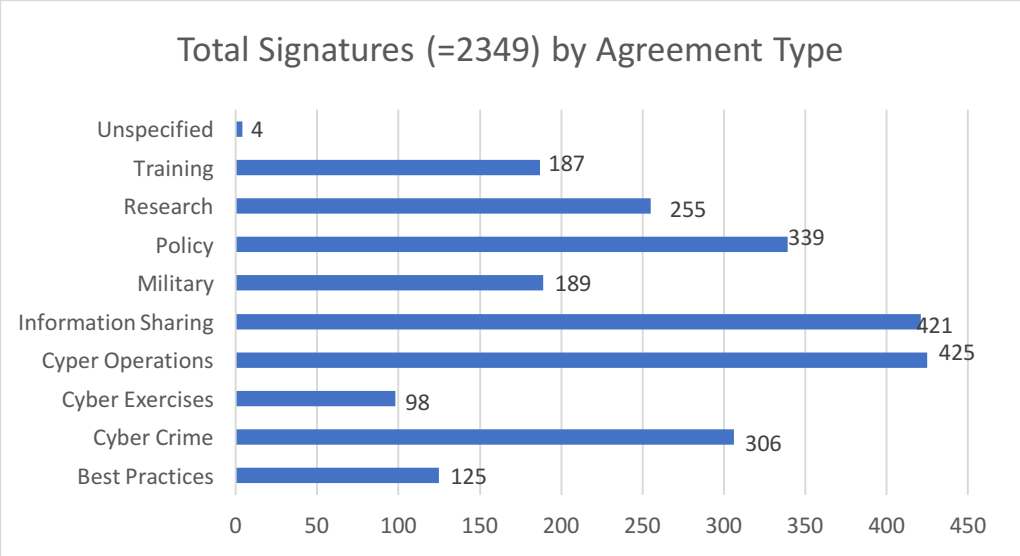
Cyber Crime – Agreements on sharing information, coordinating defenses and responses, and/or joint investigations into cyber crime incidents.

Best Practices – Agreements involving sharing of best practices for cyber protection, notifications, incident response and recovery, etc.

Any categorization scheme is bound to be somewhat subjective, and the research team found that many agreements fit multiple categories. Thus, the number of agreements by category for any given state is larger than the actual number of signed agreements. See Annex 1 on research methodology for more details.

The Military category was established to document agreements directly involving defense ministries and/or militaries, although a number of Policy and Information Sharing agreements talk in terms of sharing information on cyber defense that could involve ministries of defense or military bodies. This reflects the fact that not all nations consider cybersecurity to be a function for military forces or a national defense problem, but a problem of crime and/or internal security. For those that involve national militaries, agreement texts tend to be vague.

Overall, the bulk of activity breaks down by type as: Cyber Operations (425), Information Sharing (412), Policy (339), Cyber Crime (306), Research (255), Military (189), Training (187), Best Practices (125), Cyber Exercises (98), and unspecified (4).



This overview of agreements by type indicates that currently much cyber information sharing is at a basic level of awareness raising, as states try to improve their own national technical capabilities, policies, and approaches by learning from others. The large number of Cyber Operations agreements shows that improving technical skills is high on the agenda of many states, and reflects the existence of many CERT-to-CERT arrangements. The high number of Cyber Crime agreements is also easily explained, as crime in the cybersphere has been on the international agenda since the late 1990s and is an arena where most states have strong incentives to cooperate.

Officials involved in cybersecurity information sharing from various states have noted that much activity takes place behind the scenes or in informal settings such as conferences. For example,

states do not often publicize requests for information in the aftermath of an incident, but it is known that the U.S. government privately contacted a number of other states in the wake of the Sony hack to request forensic assistance and alerted a number of states regarding U.S. attribution of the hack to North Korea.

One impediment to international information sharing in incident response, according to numerous officials, is poor internal state coordination (a "whole of government response," as one official put it) on a timely basis. This is as true for even the most sophisticated cyber states, as well as for less advanced states. For sophisticated states, such as the United States and the U.K., the issue is setting up inter-departmental authorities, responsibilities, and accountability where many bureaucracies have "pieces" of information and partial authority, as well as different priorities. In smaller and less advanced states, the critical issue is capacity building and establishing authorities for cybersecurity. Informal conferences, often at the Track-1.5 level, are often used to both share information more freely, and to set up bilateral or small multilateral conversations.

Fewer states cooperate in the area of military activities and national security-related network protection. This is not surprising, given that secrecy regarding national security capabilities in the cybersphere is currently considered paramount, particularly as many nations seek to leverage cyber tools for offensive military operations, but it may be short-sighted. This factor weighs heavily against the success of cooperation to improve the overall level of international cybersecurity in the absence of major international incidents, because of the tension between the need to cooperate to raise the barriers to cyber exploitation by malicious actors with the need to protect one's own perceived national security requirements.

Country Levels of Activity[2]

The countries covered in this survey fall into three levels of sharing activity:

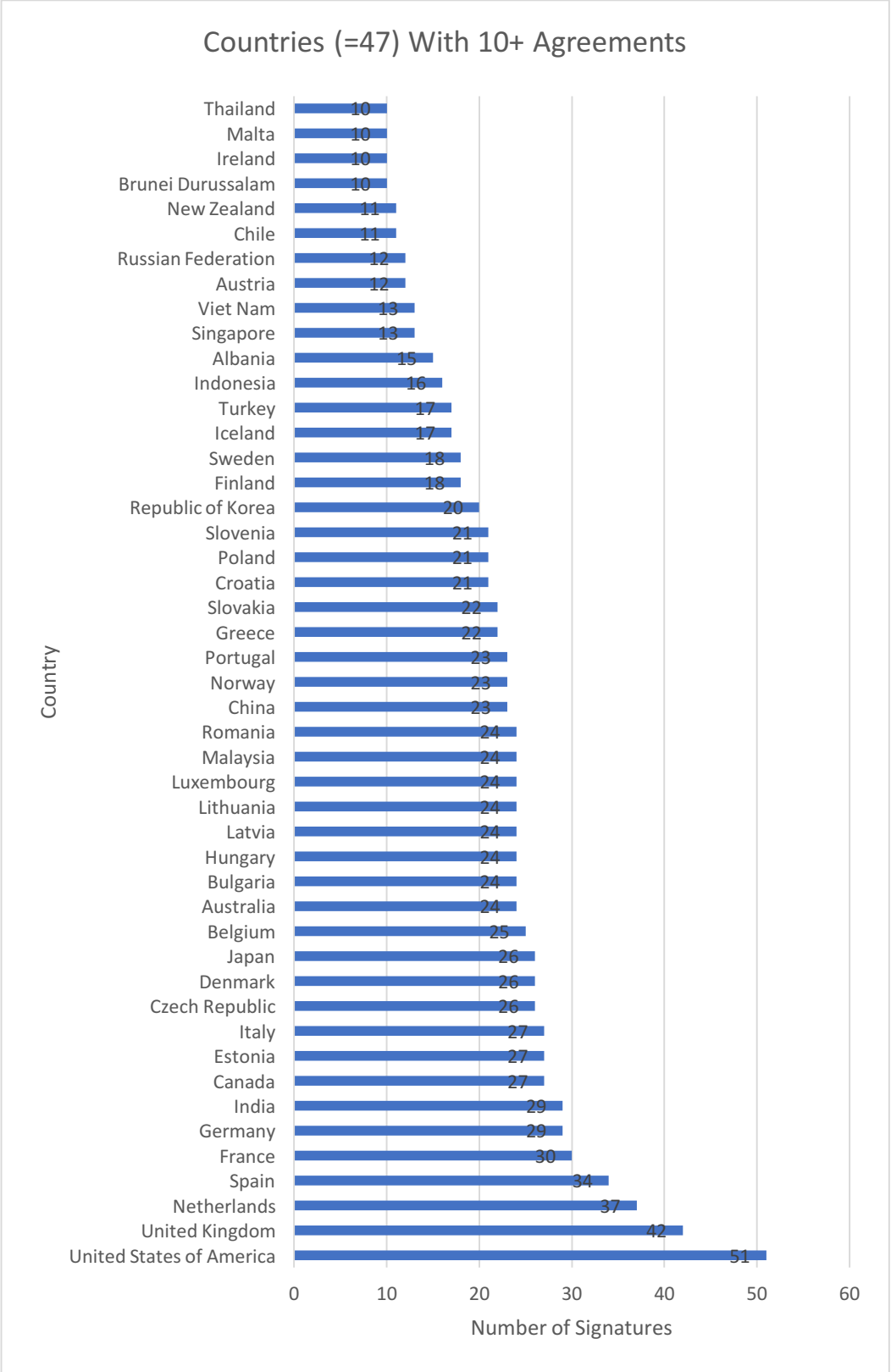
Low: The members of the largest group (71 countries) have only a few sharing arrangements each (in the single digits), generally as a member of a regional or sub-regional arrangement.

Medium: A mid-sized group of countries (40) have agreements numbering in the teens and 20s. This group is composed largely of Western countries, as well as several especially active members of ASEAN including China (23) and Japan (26). NATO members and partner countries make up the bulk of this category. One surprising member is Malaysia (24 agreements). Perhaps this is due to its status as a geographical cable hub for internet communications in the region. Another surprise is India, which has 29 agreements, despite its relative status as a newcomer to cybersecurity efforts. Russia comes in at the low end of this group, with only 12 agreements.

High: The smallest category is of "super sharers," with agreements numbering in the 30s or above. Countries in this category are: the U.S. (51), the U.K. (42), the Netherlands (38), Spain (35), and France (30). The governments of these countries have made cybersecurity a priority issue. For example, the U.K. Foreign Ministry in 2011 launched the Global Conference on

[2] Excel charts of each major country's agreements are found in the Annexes.

Cyberspace, to promote an open cyberspace; the Netherlands, another super sharer, hosted the fourth conference in 2015. Both the Netherlands and Spain have been particularly active in outreach to Middle Powers, and to developing nations in Africa and Latin America.


Countries (=47) With 10+ Agreements
Country
Thailand 10
Malta 10
Ireland 10
Brunei Durussalam 10
New Zealand 11
Chile 11
Russian Federation 12
Austria 12
Viet Nam 13
Singapore 13
Albania 15
Indonesia 16
Turkey 17
Iceland 17
Sweden 18
Finland 18
Republic of Korea 20
Slovenia 21
Poland 21
Croatia 21
Slovakia 22
Greece 22
Portugal 23
Norway 23
China 23
Romania 24
Malaysia 24
Luxembourg 24
Lithuania 24
Latvia 24
Hungary 24
Bulgaria 24
Australia 24
Belgium 25
Japan 26
Denmark 26
Czech Republic 26
Italy 27
Estonia 27
Canada 27
India 29
Germany 29
France 30
Spain 34
Netherlands 37
United Kingdom 42
United States of America 51
0
10
20
30
40
50
60
Number of Signatures

Beyond the Numbers: Cyber information sharing by and among key countries

Russia, China and the U.S.

Russia, China and the U.S., as major geopolitical competitors, have strained relationships in the cybersphere. The strains are not only based on concerns about cyber espionage for economic or political gain and potential military use of cyber tools during warfare, but also upon a fundamental philosophical disconnect. Whereas the U.S. champions free speech, global access to information, and a multi-stakeholder approach to internet governance, China and Russia are pushing for stronger "national sovereignty" in the cybersphere, meaning the right to ensure control of information content accessible to their citizens and protection of the national political sphere from outside interference via what their governments see as disruptive information. For example, while the U.S. and most Western countries use the term "cybersecurity" to discuss protection of networks and individuals from cyber intrusions, China and Russia (and some developing nations) use the term "information security" to encompass not just data protection but also content protection and use of information deemed by national laws as criminal, which can include sharing of information criticizing government policies and actions.

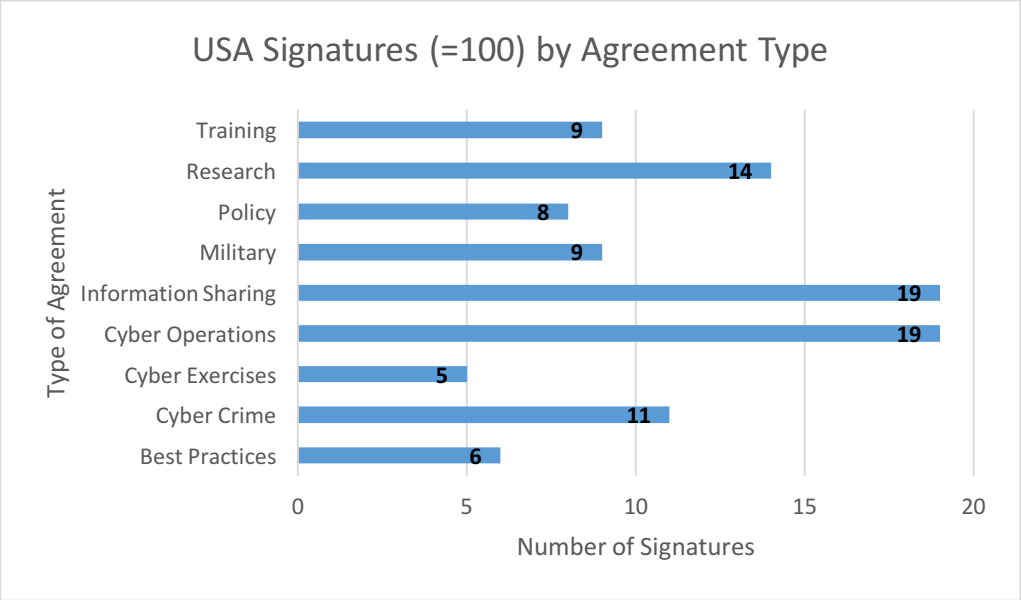
Russia and China were the architects of the Shanghai Cooperation Organization (SCO) proposal to the United Nations—introduced in 2011 and most recently updated in January 2015—for an "International Code of Conduct for Information Security" that seeks to establish an internet governance structure that lets national governments control content.[3] The Code proposal has been rejected by most Western states, due to freedom of information concerns. This ideological schism is not new to the Information Age, but reflects the longstanding tensions among differing societal constructs with regards to citizens' rights and responsibilities towards the state and the central government. At the multilateral level, this foundational gap has seen Russia and China continuing to take a leading role in promoting the concept of state control in the cybersphere in a number of fora, including at the United Nations in discussions of cyber norms of behavior under the Group of Governmental Experts on Information Security processes, within the International Telecommunication Union, and on the question of internet governance.

Cyber sharing activity among the major global powers reflects these differences in ideology and geopolitical goals. For example, likeminded Western states are the most open in sharing with each other information across all categories, including political agreements that champion human rights and freedom of information in the cybersphere. Russia, on the other hand, has limited sharing on cyber crime due to its perception that allowing outside states to be involved in investigations of criminal behavior in the cybersphere may compromise its national sovereignty. Both China and Russia have signed agreements that seek to improve their capacity, and that of other likeminded states, at the central government level to block certain information from the view of the wider citizenry.

[3] Henry Roigas, "An Updated Draft of the Code of Conduct Distributed in the United Nations: What's New?" Feb. 10, 2015, *Incyder News*, NATO Cooperative Cyber Defense Center of Excellence, https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html

United States

The United States has the largest number of cyber sharing agreements by far, with a total of 51 across the nine categories. By type, the U.S. has 100 agreements. Information Sharing, Research and Cyber Operations are the categories with the most activity, followed by Cyber Crime. There are nine agreements in the Military category, not counting the NATO Cyber Defense Policy as a whole. The U.S. has been most active over the last decade in outreach to other nations, both to achieve sharing agreements and to build capacity in the cybersphere (this includes promoting cyber literacy and use of ICTs) among allied and friendly nations. U.S. officials say that the National Security Agency (NSA) regularly informs allied countries when it detects cyber operations against them. For example, in the spring of 2017 the NSA reached out to the campaign of Emmanuel Macron during the French presidential elections after discovering suspected Russian intrusion into the campaign's operations.[4] Much of this outreach has been centered on practical cooperation rather than political cooperation, despite the fact that the U.S. is the leading promoter of the multi-stakeholder model of internet governance. As the country most invested in the internet economy, and with the most advanced domestic internet architecture, this focus on technical cooperation is perhaps to be expected.



China

China has 23 agreements in total, breaking into 45 by type with Cyber Crime, Best Practices and Information Sharing as the most common. China has 15 bilateral agreements with 12 countries—including the 2015 framework agreement with the U.S.—four of which are with Indonesia and two with Russia. The Indonesian agreements focus on cyber crime and capacity building. China has no Military agreements; however, news reports in late January 2016 cited a top Indonesian cyber official as stating that China and Indonesia would "actualize" their cyber cooperation agreements by holding cyber war simulations and crisis management exercises via a pending

[4] Adam Nossiter, David E. Sanger, and Nicole Perlroth, "Hackers Came, but the French Were Prepared," *The New York Times*, May 9, 2017, https://www.nytimes.com/2017/05/09/world/europe/hackers-came-but-the-french-were-prepared.html?_r=0

MOU with the China Cyberspace Administration.[5] The project research team could find no updated information on the reported plans.

Eight of China's 23 agreements are multilateral. China's interest in multilateral agreements has been focused on regional neighbors and organizations. Beijing has been active in ASEAN and APEC regarding cyber issues.

More recently, China has shown interest in reaching cyber sharing agreements with Western countries as well—following its agreement with the United States in September 2015 with a similar agreement (that also includes a pledge to refrain from economic espionage) with the U.K. in October 2015 and with Germany in June 2016. China's state-owned internet company Huawei in February 2016 signed its first agreement with a Western country, Spain. The agreement with the Spanish National Institute of Cybersecurity (INCIBE) calls for the sharing of cyber protection and best practices, and includes the training of Spanish technologists. It also has a CERT-to-CERT agreement with Australia, and an agreement with South Korea dating from 2014 that covers joint response to cyber incidents such as DDoS attacks and information sharing on threats.[6]

China has two bilateral agreements with Russia and is a signatory to the SCO agreement. These agreements focus on establishing state control in the cybersphere, preventing "information crimes," and the sharing of technology aimed at content monitoring and protection of internal networks from information deemed malicious. The overarching China-Russia agreement was

[5] "Indonesia-China to actualize cooperation on cyber defense," *Antara News*, January 23, 2016, http://www.antaranews.com/en/news/102710/indonesia-china-to-actualize-cooperation-on-cyber-defense; Greg Austin, "China and Indonesia: Joint Cyber War Simulations," *The Diplomat*, January 28, 2016, https://www.eastwest.ngo/idea/china-and-indonesia-joint-cyber-war-simulations

[6] "Korea, China to upgrade cooperation in ICT, cyber security," *KoreaNet,* http://www.korea.net/NewsFocus/Sci-Tech/view?articleId=109797

signed in April 2015, and covers "cooperation in the field of international information security."[7] The agreement's preamble lays out some concerns and motivations for the agreement, such as:

> Expressing concern for the threats related to the use of such technologies in the civilian and military purposes not inconsistent with the objectives of international peace, security and stability, with the goal of undermining the sovereignty and security of states and interfering in their internal affairs and violating the privacy of citizens, destabilizing the political and socio-economic environment, stirring up national and religious hatred;
>
> Attaching great importance to international information security as to one of the key elements of the system of international security;
>
> Reaffirming that the sovereignty and international norms and principles, arising from state sovereignty, apply to the conduct of states in the framework of the activities …

This is a wide-ranging agreement that includes joint responses to threats, cooperation on critical infrastructure protection, cooperation between the technical authorities for computer emergency response, information sharing on potential risks and threat assessment, and cooperation on political action within international organizations including the United Nations.

The second agreement, made at the same time, is between Kaspersky Lab and Zhongguo Wangan, a division of the state-run China Electronics Technology Group Cooperation (CETC), for cooperation on software to prevent cyber attacks.[8] The deal is for Kaspersky Lab to assist China in building up malware protection software.

In line with its concerns regarding government control over content and "information warfare," since 1998 China has been building its so-called "Great Firewall," to screen and block incoming internet content. This includes blocking access to major websites such as Google and Facebook, and attempting to substitute such sites with domestic websites (Baidou for Google and Weibo for Facebook) that are monitored closely by security services. China's parliament passed a new law in November 2016 aimed at cracking down on the hacking of Chinese government and industry networks, and it sparked protests from human rights activists and foreign businesses active in China. The most controversial provisions of the law include requirements for "critical information infrastructure operators" to store personal information and business data in China, provide "technical support" to security agencies, and pass national security reviews in order to continue operations.[9]

Russia

Russia has entered in 12 total cyber sharing agreements, 29 when broken down by type, with the biggest category being Information Sharing. Russia has bilateral agreements with only eight countries. Only one Russian agreement falls directly into the Military category, a bilateral

[7] See: http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf; CISSM has an unofficial translation in English (Annex 2) and the Russian-language version of the agreement is in Annex 3.
[8] "Kaspersky Lab to Cooperation with China's Zhongguo Wangan," TASS, Dec. 17, 2015, http://tass.com/economy/844712
[9] "China's new cybersecurity law sparks fresh censorship and espionage fears," *Reuters*, Nov. 7, 2016, https://www.theguardian.com/world/2016/nov/07/chinas-new-cybersecurity-law-sparks-fresh-censorship-and-espionage-fears

agreement with Iran that includes exchanges of intelligence information, interaction against threats, and joint defense activities.[10] Interestingly, Russia has two separate agreements with Japan, dating from 2013 and 2014, which fall into the categories of Training and Information sharing with a particular eye on working cooperatively in ASEAN.

Russia has very little interaction in the category of Cyber Crime—which overall is one of the largest categories by the number of signatures documented by the project team. Moscow has only three such agreements, with India, Iran and the SCO. This is reflective of Russia's animosity toward allowing other nations to assist in tracking down Russian-based cyber criminals, allowing Interpol access in case of cross-border crimes, and the Budapest Convention of 2001 (the first treaty on cyber crime, developed by the Council of Europe) due to concerns regarding national sovereignty.

Cooperative efforts between Russia and the United States, which resulted in a package of agreements in 2013, were suspended in the wake of the Ukraine crisis. However, Russian and U.S. representatives met in April 2016 in Geneva to attempt to revitalize cooperation[11].

Russia has also been active in cyber cooperation discussions at APEC (signing three agreements), which are largely aimed at improving capabilities in the region, but also include cooperation to fight spam.

According to Russian cyber security experts,[12] the most important relationship for Moscow in the cybersphere is with China. These sources said that the Kremlin has been seeking to emulate

[10] "Iran, Russia Agree on Cyber-Defense Cooperation: Official," *Tasnim News Agency,* June 13, 2015, https://www.tasnimnews.com/en/news/2015/06/13/768309/iran-russia-agree-on-cyber-defense-cooperation-official
[11] Evan Perez, "U.S. and Russia meet on cybersecurity," April 17, 2016, *CNN.com*, http://www.cnn.com/2016/04/17/politics/us-russia-meet-on-cybersecurity/

China's "Great Firewall" to allow the government to—if deemed necessary to protect Russia from those seeking to undermine the government and/or society—withdraw from the World Wide Web completely. Russian efforts are aimed at creating the technical capabilities for "autonomy," for example by switching all "names" in the .ru and .rf databases to an internal server, in order to "cut Russia off" from the global Domain Name System if the government decides that "threats" require this.

The Kremlin's efforts to tighten control over the internet are spearheaded by Igor Shchyogolev, long-time associate of President Vladimir Putin and currently special assistant on internet issues. In November 2016, his proposal to put Russian top-level domains (TLDs) under government control via regulations on access providers was translated into legislation that includes federal government control of all cross-border fiber optic cables transmitting internet information.[13] This follows the enactment of the so-called "Yarovaya Law," cracking down on "promotion of terrorism" in cyberspace—with punishment of up to seven years in prison for violation. The law also requires telephone and internet providers to store all communications data for six months, and all metadata for three years.[14] These experts noted that Russian company Bulat, a subsidiary of state-owned Rostec, has been negotiating with China's Huawei for licensed production of its data storage software, although so far there have been no reports that a deal has been struck.[15] Russia's relationship with China on cyber issues is primarily aimed at improving Russian technology, according to these sources, as well as promoting internet sovereignty in the international arena.

Experts in Moscow said that Shchyogolev's plans also include establishing a "white list" of "safe" websites—as opposed to the current Russian practice of blacklisting certain websites such as LinkedIn—something that has been promoted by the Safe Internet League, a lobby organization promoting the use of internet filters and that is suspected of being an arm of the Russian security services. The Safe Internet League in December 2015 signed a cooperation agreement with the Cybersecurity Association of China, subsequent to the 2015 Wuzhen Conference on Internet governance, the theme of which was the need for a "new model" to establish government control over the internet.[16] In May 2017, Russian President Vladimir Putin signed an executive order that seeks to put new controls on online media outlets and crack down on online anonymity. It also instructs that all federal agencies replace all imported software and computer equipment with domestic equivalents.[17]

---

[12] Interviewed in Moscow in late September 2016.

[13] Andrei Soldatov and Irina Borogan, "Putin brings China's Great Firewall to Russia in cybersecurity pact," *The Guardian*, Nov. 29, 2016, https://www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact

[14] Alec Luhn, "Russia passes 'Big Brother' anti-terror laws," *The Guardian*, June 26, 2016, https://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother-anti-terror-laws

[15] "Russia in Talks with China's Huawei on Data Storage Technologies' Licensing," *Sputnik News*, Aug. 24, 2016, https://sputniknews.com/science/201608241044578435-russia-huawei-bulat-data/

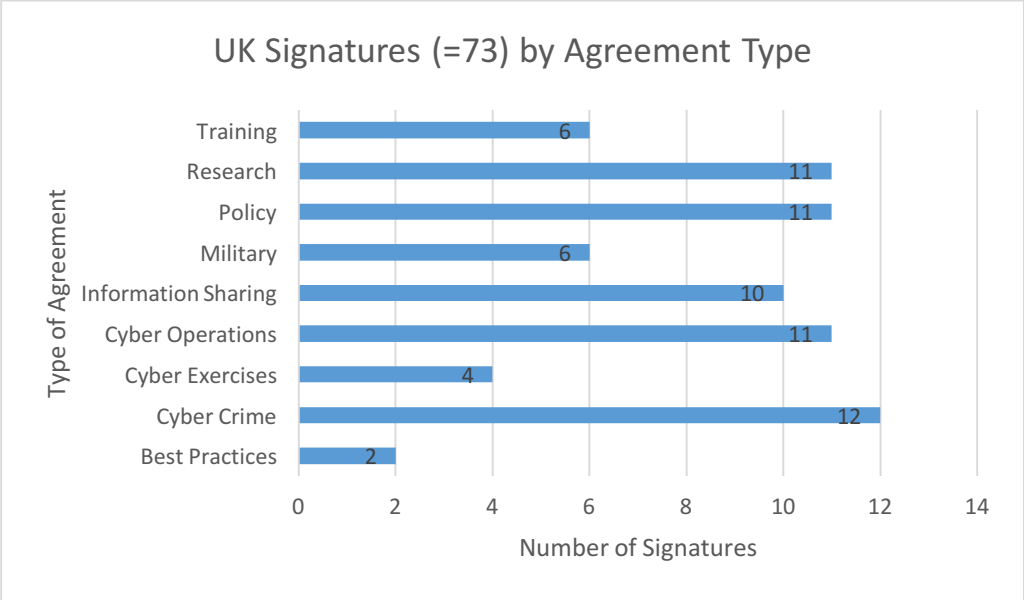
[16] "Cooperation Agreement signed by Russia's Safe Internet League and China's Cybersecurity Association," Safe Internet League press release, Dec. 22, 2015, http://www.ligainternet.ru/en/news/news-detail.php?ID=13017

[17] "Executive Order Cracks Down on Internet Media and Online Anonymity," *The Moscow Times*, May 15, 2017, https://themoscowtimes.com/news/putins-new-executive-order-cracks-down-on-internet-media-and-online-anonymity-57970; "Russia approves information society development strategy through 2030," *Medusa Project*, May 10, 2017, https://meduza.io/en/news/2017/05/10/russia-s-approves-new-information-society-development-strategy-through-2030

These experts noted that concerns about the crackdown on Internet freedom has led to an upsurge in Russian use of TOR and VPN services over the last year, and is spurring concerns from Russian industry regarding possible effects on the economy and trade already suffering due to Western sanctions.

United Kingdom

The U.K. has the second largest number of cyber sharing agreements at 42, breaking down into 73 by type. The largest category, Cyber Crime, at 12; followed by Policy, Research and Cyber Operations at 11 each. Ten of the agreements cover Information Sharing; six cover Military cooperation. Britain has been active in cybersecurity sharing activities for much of the past decade, with most of those activities taking place in the multilateral arena via NATO and the European Union. London has signed 15 bilateral agreements, including several in Southeast Asia and one with Qatar.



In November 2016, the British Government released a new cybersecurity strategy for the next five years, pledging to invest 1.9 billion pounds in defending British cyber infrastructure. The objectives of the new policy are stated as: "defend, deter, and develop," and include a focus on international action. The British policy includes a direct embrace of offensive actions to "deter" and "respond to" attacks. Cybersecurity operations were centralized under the National Cyber Security Centre in October 2016, which is a sub-unit of Britain's spy agency, the GCHQ. In the international arena, a key goal is to "strengthen and embed a common understanding of responsible state behavior in cyberspace."[18]

[18] "National Cyber Security Strategy 2016-2021," Her Majesty's Government, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Britain traditionally has fewer domestic legal protections for individual privacy regarding GCHQ activities and stronger government abilities to censor information for national security reasons than does the U.S. With that underlying philosophy in mind, the U.K. government is taking a strong centralized role in cybersecurity. Indeed, at a cybersecurity conference in Washington, D.C. in September 2016, the head of cybersecurity at GCHQ, Ciaran Martin, said that one of the agency's new "flagship programs" will be to build a national firewall to protect consumers. "What better way of providing automated defenses at scale than by the major private providers effectively blocking their customers from coming into contact with known malware and bad addresses?" Martin said.[19]

The Netherlands

The Netherlands, the smallest of the super-sharing countries, has been disproportionately active in multilateral and multi-stakeholder forums. It has been routinely briefing delegations to the Conference on Disarmament in Geneva about its cyber policies and activities. It also financially supported the effort by the NATO Cooperative Cyber Defence Centre of Excellence, in Tallinn, Estonia, to develop a consensus view of the application of international law in the cyber domain. In 2015, the Netherlands established the Global Forum on Cyber Expertise to identify best practices related to cybersecurity, cyber crime, data protection and e-governance. The forum currently has 56 members and is open to countries, companies and intergovernmental agencies that support the Hague Declaration that established the group.[20] In February 2017, the Dutch government initiated a partnership with Microsoft and the East-West Institute to stand up the Global Commission on the Stability of Cyberspace, an independent, multilateral commission to develop proposals for norms and policies to enhance international cybersecurity.[21] The Commission will fund researchers around the globe, as well as support multilateral processes and undertake capacity building.

India

India has rapidly ramped up its cyber sharing activity recently. It had no cybersecurity policy until 2013, but New Delhi has been scrambling since to protect both its networks and its public as the use of mobile phones and social media continues to rise rapidly. India's key preoccupation, according to Indian diplomats, is to ensure safe online access to the Indian public, and elsewhere in the developing world. In addition, India has been trying to encourage the development of widespread electronic banking and payment capabilities; activities that require a high degree of confidence in the security of data passed through the cybersphere.

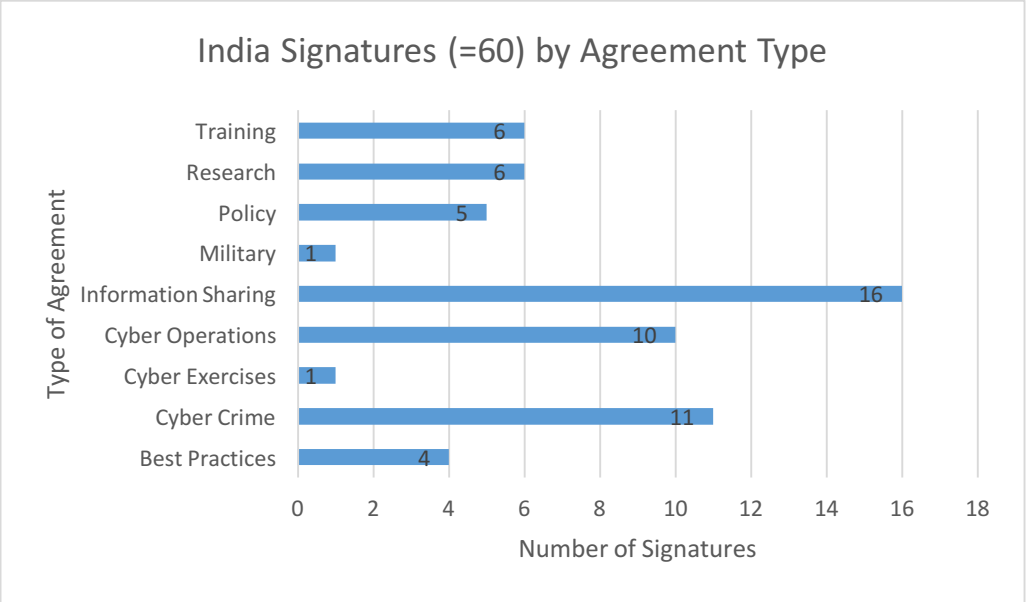
India has signed a total of 29 agreements, 60 when broken down by type:16 Information Sharing agreements; 10 Cyber Operations agreements; 11 Cyber Crime agreements; 6 Research agreements; 6 Training agreements; 5 Policy agreements; 4 Best Practices agreements; 1 Cyber Exercise agreement; and 1 Military agreement. The Military agreement is with the United States, in part of an accord signed in January 2004 following their joint cyber forum. The agreement established five joint working groups to cover legal cooperation and law enforcement, research and development, critical information infrastructure, watch and warning emergency response,

[19] Matthew Reynolds, "GCHQ wants to protect the UK from cyberattacks with a government firewall," *Wired*, Sept. 14, 2016, http://www.wired.co.uk/article/gchq-firewall-private-companies
[20] See: https://www.thegfce.com/
[21] See: https://cyberstability.org/

military cooperation and standards and software assurance. India has signed a total of six agreements by type with the United States, and four with Russia—two focused on cyber-terrorism, with one specifically aimed at monitoring ISIL activities online; and two focused on "sustainable global use of ICTs."[22] Four of India's bilateral agreements involve CERT-to-CERT cooperation, and one (with Malaysia) involves CERT-to-Cyberagency cooperation. India further will host the Global Conference on Cyberspace in late 2017, a semi-formal, high-level meeting of government, industry and civil society representatives that has taken place biannually since 2011 on a routine basis.

India is still wrestling with setting up a government framework for cybersecurity, partly due to debate within the country about how much power the Indian government should have over use of the Indian cyber network. India's Union Party government has expressed sympathy for the Russia/China argument regarding the need for national sovereignty in content control.

Indeed, India's agreements with Russia reflect typical Russian language about "national sovereignty" in the cybersphere and concerns about cyber "misinformation." At the same time, India's agreements with the U.S. tout "freedom of information" in the cybersphere. Indian officials reject criticism that its political stance at the international level is contradictory; rather,



officials contend that Delhi is taking a "flexible" approach that allows it to craft an "Indian" policy that will in some way straddle these two polar approaches.

For its part, India's high-tech sector has pushed back on efforts at tighter centralized controls on information. For example, in September 2015, after widespread opposition from tech companies, the government was forced to withdraw a draft law that would have required the storage of plain

[22] "Druzhba-Dosti: A Vision for Strengthening the Indian-Russian Partnership over the Next Decade' - Joint Statement during the Visit of President of the Russian Federation to India," Indian Ministry of External Affairs Press Release, Dec. 11, 2014, http://pib.nic.in/newsite/PrintRelease.aspx?relid=113166 Unfortunately, the term "sustainable development of ICTs" is not defined.

text and outlawed all but government approved encryption algorithms.[23] Blocking Internet access also has become a common and controversial practice by some Indian states as a measure against terrorism and political violence.[24]

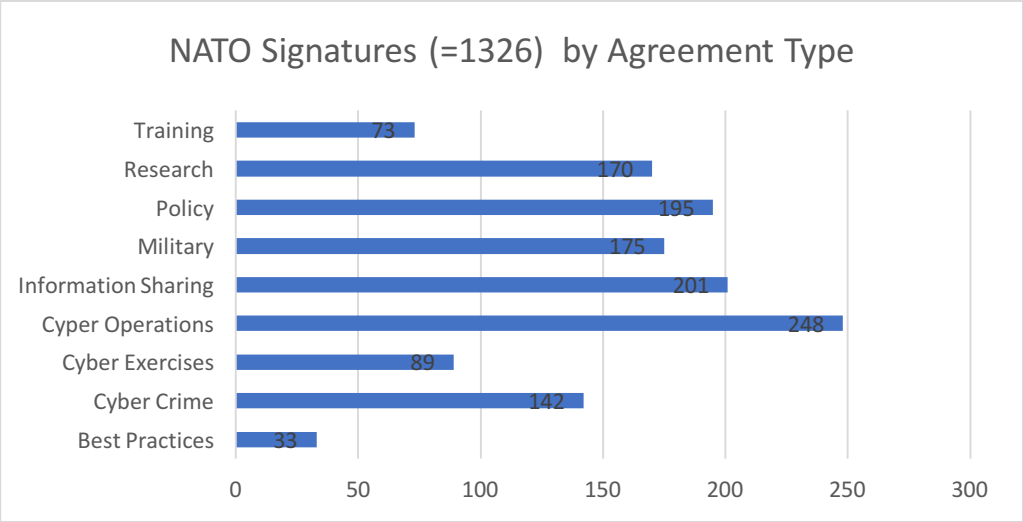
Regional Activity

As Western states are the most active at the national level in cybersecurity sharing, regional organizations involving those states also show more activity. For instance, ASEAN nations among themselves have 236 agreements by type, whereas the ASEAN Regional Forum (ARF), which involves the United States and several other Western allies, has 1,862 agreements by type. Despite the difference in size of the organizations (ASEAN, 10 States; ARF, 27 States), the extent of sharing among ARF members is significantly greater.

NATO

NATO is the most active regional organization on cybersecurity, and in particular, cyber defense. As a military alliance, NATO differs from other regional organizations in having a collective infrastructure to underpin joint military operations, including command and control networks that require cyber protection. In addition, NATO members are wedded to assisting each other in improving cyber defenses for national militaries.

NATO countries account for a total of 1,326 agreements by type, with the largest category being Cyber Operations.



[23] Jim Edwards, "India scraps its proposal for a completely bonkers encryption law that required plain text storage," *Business Insider*, Sept. 22, 2015, http://www.businessinsider.com/india-encryption-law-requires-plain-text-storage-2015-9

[24] Samir Saran, Bedavyasa Mohanty, "Cyber (In)Security in India," Feb. 16, 2016, *LAWFARE*, https://www.lawfareblog.com/cyber-insecurity-india

NATO began official efforts on cybersecurity in 2002, as a political decision of the Prague Summit, aimed at protection of NATO's collective information systems and has been extremely active since—partly piqued by the attacks on Estonia in 2007. Following the cyber attacks against Estonia in 2007, NATO approved its first Policy on Cyber Defense in January 2008, which was updated in June 2011. Critically, the NATO Defense Planning Process integrated cyber defense into NATO defense requirements in April 2012, laying out priorities and requirements for individual member states in their defense planning. The current NATO cyber defense policy dates from September 2014, and in June 2016 NATO defense ministers declared cyberspace as a specific domain of allied military operations—along with land, sea, and air.[25]

In October 2016, NATO for the first time appointed an intelligence chief, creating the post of assistant secretary-general for intelligence and security.[26] While the post is primarily aimed at combining military and civil intelligence regarding terrorism, a source involved in NATO's cybersecurity activities said that it also will include intelligence gathering regarding cybersecurity. In addition, this source said, Supreme Headquarters Allied Command Europe (SHAPE) has created a new Task Force on Cyber, with about 60 full-time slots, headed by USAF Col. Ali Rizwan.[27]

Despite the robust nature of NATO's efforts to create new structures, policies and operational guidance on cyber defense, a number of sources have said that at the operational level, much remains unclear, overly complicated, or simply not working. A particular problem faced by NATO is that there is little clarity about how the Supreme Allied Commander Europe (SACEUR)—one of NATO's two strategic commanders responsible for military operations in Europe and always a U.S. officer—collaborates with NATO member states. There are no set procedures for such issues as de-conflicting NATO and member-state operations, for example.

Another issue is the continued political tension within NATO about the use of offensive cyber operations, which some member states have embraced. The fact that a small group of NATO members and NATO partners—the so-called Five Eyes, led by the United States and including Australia, Canada, New Zealand and the United Kingdom—have much more intensive intelligence sharing among themselves than with NATO writ large, including cooperation on cybersecurity and an interest in cyber offense, has raised tensions within the Alliance. In an example of the problems surrounding cyber offense, there was a fierce internal debate in the United States in late 2016 about whether to inform allied countries about a Pentagon-led campaign to disrupt Islamic State recruitment/propaganda websites that were hosted on computers in allied countries. The debate pitted Cyber Command and the Joint Chiefs of Staff—who argued that they not only had the authority to conduct such operations without notifying allies, but also that notification might undercut the campaign through leaks—against the CIA, the FBI, the State Department, and the Director of National Intelligence, who were concerned about

[25] For background and history of NATO's cyber defense activities and policies, see NATO's website: http://www.nato.int/cps/en/natohq/topics_78170.htm

[26] Julian Barnes, "NATO Appoints Its First Intelligence Chief," The Wall Street Journal, Oct. 21, 2016, https://www.wsj.com/articles/nato-appoints-its-first-intelligence-chief-1477070563

[27] Interview Jan. 10, 2017. The source has been involved officially with NATO's efforts to improve its cybersecurity structures and operations. For a presentation by Col. Rizwan on NATO's cybersecurity structure and operations, given at Australian Defense Magazine's Cyber Security Summit 2016 in Canberra, Australia, see: http://www.slideshare.net/informaoz/col-rizwan-ali-us-air-force

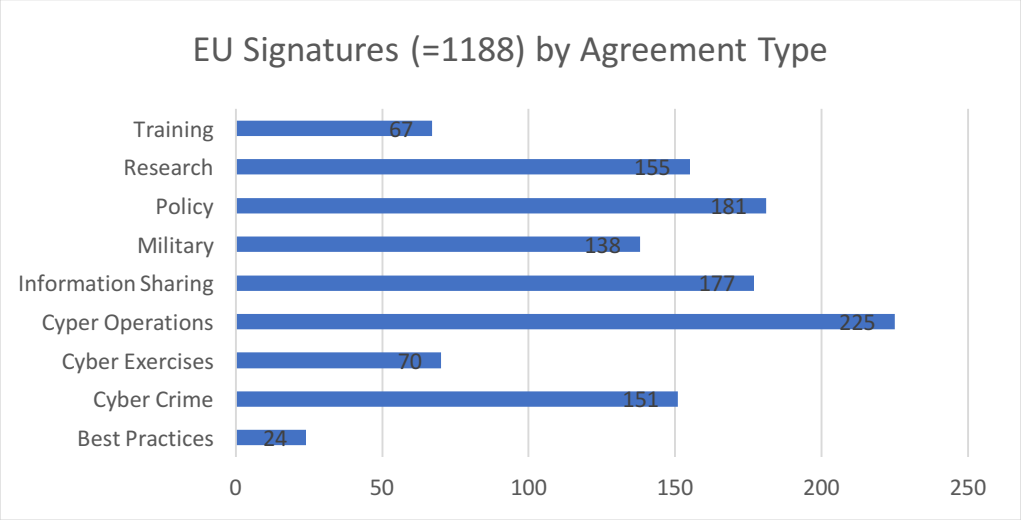
blowback if allies were not notified. In the end, notification was given to those countries where the operations took place.[28]

Even more complicated is the question of NATO relations with the European Union on cybersecurity issues: Although there is a relatively new (February 2016) "Technical Arrangement" on cyber defense between the EU and NATO that is in essence a CERT-to-CERT agreement,[29]sources say there are no day-to-day processes for communications and that much is dependent on personal relationships.

Lastly, the relationship between SACEUR (who also commands cyber defense operations) and the NATO Communication and Information Agency (NCIA) is convoluted in the extreme. NCIA, located in Brussels, was established to provide ICT services and is essentially a private contractor (it is a fee-paying business) that SACEUR has no real control over or insight into regarding its activities in building networks, providing connectivity services, etc. This means, for example, that if an expeditionary operation were undertaken under SACEUR's command, he/she would not necessarily control the architecture of the ICT network in the field, nor have any idea how to fulfill the mandate to provide cyber defenses for it.

EU

EU countries account for signatures on 1,188 agreements by type, with the largest categories being Cyber Operations (225), Policy (181) and Information Sharing (177). Interestingly, Best Practices agreements only number 24 and Cyber Exercises number 70.



[28] Ellen Nakashima, "U.S. military cyber operation to attack ISIS last year sparked heated debate over alerting allies," *The Washington Post*, May 9, 2017, https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.1eabf6c8513b

[29] "EU and NATO cyber defence cooperation," EU External Action Service Fact Sheet, Feb. 10, 2016, http://collections.internetmemory.org/haeu/content/20160313172652/http://eeas.europa.eu/top_stories/2016/100216_eu-nato-cyber-defence-cooperation_en.htm

The European Commission signed a Cybersecurity Strategy of the European Union on July 2, 2013. The strategy was designed to clarify the role of the EU (rather than that of the member states working together through the EU Council) in protecting the cyber domain, and set forth a series of "actions" to be taken by the EU. These "actions" include:

- achieving cyber resilience, by increasing capabilities, preparedness, cooperation, information exchange, and awareness in the field of Network and Information Security, for the public and private sectors and at national and EU level;
- drastically reducing cybercrime by strengthening the expertise of those in charge of investigating and prosecuting it, by adopting a more coordinated approach between law enforcement agencies across the Union, and by enhancing cooperation with other actors;
- developing an EU Cyber Defence Policy and capabilities in the framework of the Common Security and Defence Policy;
- fostering the industrial and technological resources required to benefit from the Digital Single Market. This will help stimulate the emergence of a European industry and market for secure ICT; it will contribute to the growth and competitiveness of the EU economy; and it will increase the public and private spending on cybersecurity research and development (R&D);
- enhancing the EU's international cyberspace policy to promote EU core values, to define norms for responsible behaviour, to advocate the application of existing international law in cyberspace and to assist countries outside the EU in building cybersecurity capacity.[30]

A large part of the EU effort is centered on increasing the capacity of the 28 member countries and creating a level playing field in European cyberspace. To do this, the EU Council signed, and the Parliament ratified, the "Directive on Security of Networks and Information Systems (NIS Directive)" in July 2016, which lays out member country responsibilities and sets up cooperative mechanisms. Under this directive, all member countries must establish a Computer Security Incident Response Team (CSIRT), and enable them to work together through a CSIRT Network. It establishes a Cooperation Group to manage cooperation, as well as encourages members to work through the European Union Agency for Network and Information Security (ENISA) that was established in 2004 in Greece as a center of excellence in supporting EU members to improve cybersecurity.[31] The Cooperation Group will consist of representatives of member countries, the European Commission and ENISA, with the Commission acting as the secretariat. It is charged with facilitating information sharing on risks, incidents, awareness-raising, training and research and development.[32] The directive further encourages nations to notify the secretariat of the CSIRT Network regarding incidents, and that this information should

[30] "Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace," European Commission, July 2, 2013, https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace.
[31] European Union Agency for Network and Information Security website: https://www.enisa.europa.eu/about-enisa
[32] "Directive on Security of Network and Information Systems," European Commission Press Release, July 6, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

be housed on a website available to all.[33] Importantly, digital service providers such as search engines and cloud services that cross borders are obligated to provide such notice.[34]

As noted above, in February 2016, the EU signed a Technical Arrangement with NATO to improve cyber incident prevention, detection, and response in both organizations. The EU and NATO began efforts to coordinate on cybersecurity in 2010, and to have annual high-level meetings. The EU also participates as an observer in NATO's annual Cyber Coalition exercises.[35] However, according to officials familiar with the situation, cooperation remains spotty and largely unclarified.

The EU has been active as well in outreach to non-EU members for capacity building since 2010, beginning with efforts on cyber crime. Efforts are now focused on building up legal structures and technical capabilities in third-party states.[36]

SCO

The Shanghai Cooperation Organization (SCO) was formed in 2001 as a forum for regional confidence building. Member states include China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan. India and Pakistan began the process of acceding to the organization in 2015 and were accepted as members in June 2016 at the SCO summit in Tashkent.[37] However, they are not expected to become full members until 2017. Meanwhile, Iran, currently an observer state, is next in line.[38] There are three other observer states: Belarus, Mongolia and Afghanistan. The SCO also has so-called dialogue partners: Armenia, Turkey, Sri Lanka, Nepal and Cambodia. Over time the SCO's mandate has been widened to include military cooperation, counterterrorism, and intelligence sharing.

The SCO countries account for a total of 99 signatures by agreement type. The bulk of these agreements are in the Information Sharing, Crime, and Policy categories. There are no agreements that include joint Cyber Exercises, and only five that cover Best Practices.

---

[33] "DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," *Official Journal of the European Union*, L 194/1, 19/7/2016, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

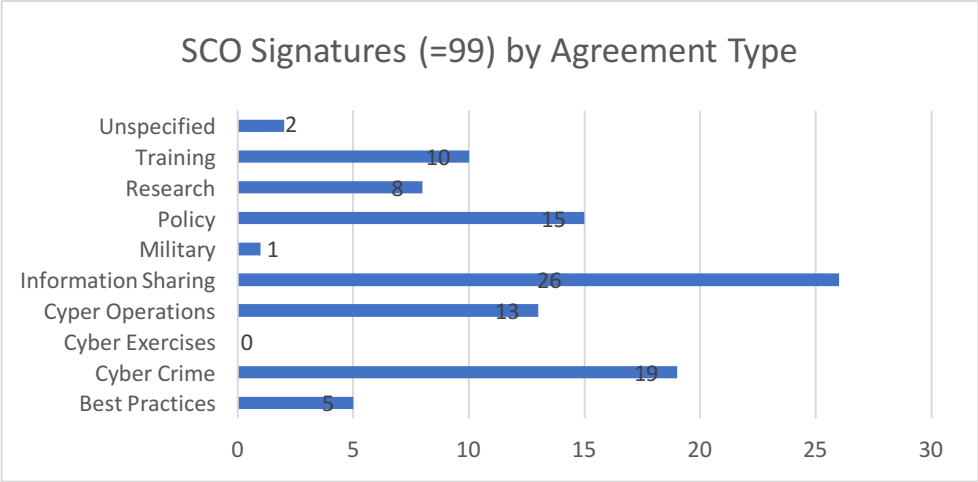
[34] Tom Reeve, "New EU directive requires critical infrastructure to improve cyber-security," *SC Media*, July 6, 2016, https://www.scmagazineuk.com/updated-new-eu-directive-requires-critical-infrastructure-to-improve-cyber-security/article/530778/

[35] "EU and NATO cyber defence cooperation," European Union External Action Service, Feb. 10, 2016, http://collections.internetmemory.org/haeu/content/20160313172652/http://eeas.europa.eu/top_stories/2016/100216_eu-nato-cyber-defence-cooperation_en.htm.

[36] Panagiata-Nayia Barmpaliou, "The EU Experience in Global Cyber Capacity and Institution Building," Global Forum on Cyber Expertise website, June 20, 2016, https://www.thegfce.com/news/news/2016/06/20/eu-experience-in-global-cyber-capacity

[37] "Admission of India, Pakistan makes SCO very powerful – Putin," *Interfax*, June 23, 2016, https://rbth.com/international/2016/06/23/admission-of-india-pakistan-makes-sco-very-powerful-putin_605445

[38] Peter Korzun, "Shanghai Cooperation Organization: Story of Success and Expansion," *Strategic Culture*, June 29, 2016, http://www.strategic-culture.org/news/2016/06/29/shanghai-cooperation-organization-story-success-expansion.html



The SCO agreement on "Cooperation in the Field of Ensuring International Information Security" was signed in 2009 by Russia, China, Kazakhstan, Tajikistan, Uzbekistan, and Kyrgyzstan.[39] It is unclear whether Pakistan and India are considered adherents to the pact with their accession agreements to the SCO.

The agreement pledges the parties to work together to counter threats in the "information" sphere, which are detailed as follows:

1. Development and use of information weapons, preparation for and waging information war;
2. Information terrorism;
3. Information crime;
4. Use of the dominant position in the information space to the detriment of the interests and security of other states;
5. Dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other states;
6. Natural and/or man-made threats to the safe and stable operation of global and national information infrastructures.[40]

The agreement includes a pledge to jointly monitor and respond to threats, to collaborate to strengthen the "information security" of the partners, and to implement coordinated policies and technical standards for using "the electronic digital signature and information protection" in trans-border information exchange. It also calls upon the signatures to work together in the international arena to develop "norms of international law" to "curb the use of information weapons," and to influence international organizations. It does not, however, specify measures for actually sharing information about cyber threats and response, leaving the development of practices and methods to individual signatures via bilateral accords.

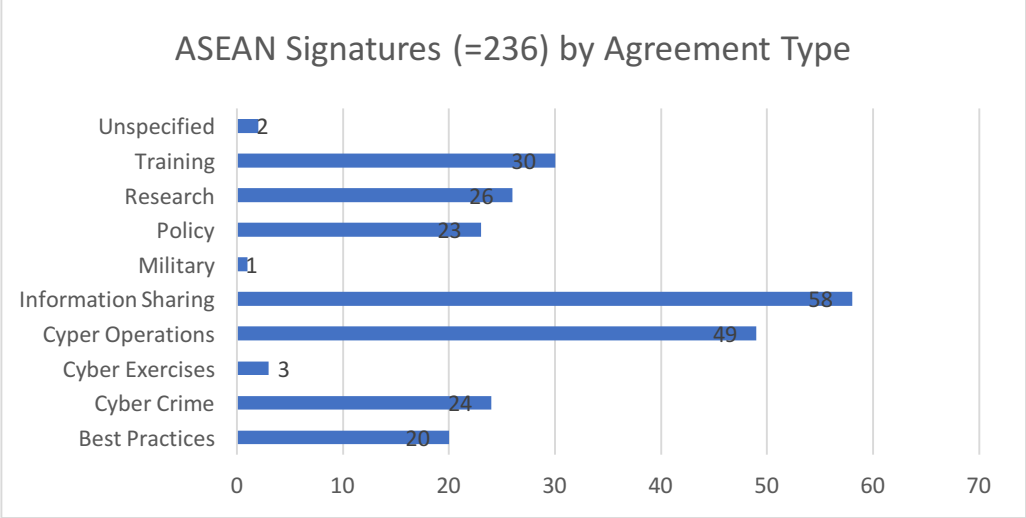
Although cybersecurity has been an ongoing topic at SCO summits, Russian cyber experts say the group's activity does not include much by the way of actual cybersecurity sharing. Instead, the organization's main purpose seems to be political, aimed at influencing states to join the

[39] Russian text found here: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf
[40] See Russian original in Annex 4; Unofficial English translation in Annex 5

Code of Conduct proposal and to work with the SCO to push sovereignty-based internet governance that allows content control. For example, Russia's only SCO partner in a bilateral agreement is China. China has bilateral agreements with only Russia, Tajikistan, and India. Kazakhstan has a total of six agreements; Kyrgyzstan has one; and Uzbekistan and Tajikistan have three agreements apiece.

ASEAN/ARF

The Association of Southeast Asian Nations (ASEAN) has 10 members: Brunei, Cambodia, Indonesia, Lao, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam. ASEAN countries cooperate across many domains, with the central purpose of promoting regional economic growth. Political and security issues, including confidence building and conflict prevention, are discussed under the auspices of the ASEAN Regional Forum (ARF), established in 1994. It has 27 members, which, in addition to the 10 ASEAN states, include: Australia, Canada, China, the European Union, India, Japan, New Zealand, the Republic of Korea, Russia, and the United States. Meetings take place at the level of Foreign Ministers. ASEAN members account for 236 signatures on agreements by type, with the largest categories being: Information Sharing (58), Cyber Operations (49), and Training (30).

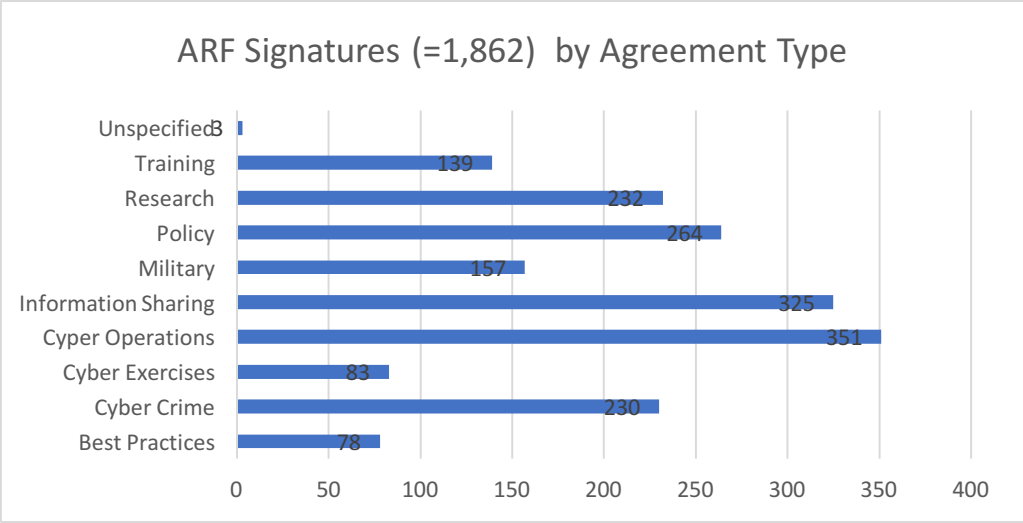


ARF members account for 1,862 signatures on agreements by type, with the largest categories being Cyber Operations (351) and Information Sharing (325). Given the inclusion of the United States, EU members, and China in ARF, the level of activity is understandable.
In October 2015, the United States and Singapore co-sponsored a seminar in Singapore on cybersecurity to follow up the approval of the "ARF Work Plan on the Security of and in the Use of Information and Communications Technologies" on Aug. 6, 2015 at the 22nd ARF Ministerial.[41] The plan, which was drafted by Australia, Russia and Malaysia, is focused on building confidence in the region regarding cybersecurity. Among its goals are to establish information sharing about cyber threats, develop a common lexicon, and establish a regional

[41] U.S. Ambassador to Singapore Kirk Wagar, "Welcoming Remarks on the ARF Seminar on Operationalizing Cyber Confidence-Building Measures," Oct. 21, 2015, https://singapore.usembassy.gov/arf-seminar102115.html

network of points of contact.[42] ASEAN subsequently held its first ministerial conference on cybersecurity on October 11, 2016 in Singapore. Foreign ministers agreed on the need to further institutionalize ASEAN cooperation and coordination on cybersecurity.[43]

ASEAN also has conducted 11 annual ASEAN CERTS Incident Drills—exercises among the national CERTS and the Asia-Pacific Computer Security Response Team.[44] In May 2016, the



ASEAN Defense Ministers Meeting decided to create a new Experts Working Group on cybersecurity under the ADMM-plus (the group of ASEAN defense ministers plus those of the eight official "dialogue" countries).[45] The proposal was crafted by the Philippines, and the working group will be co-chaired by the Philippines and New Zealand from 2017-2020.[46]

Cybersecurity cooperation in Asia is complicated by the varied security and defense ties of the nations involved, and the difference in membership between ASEAN and ARF. Many ASEAN nations seemingly lean toward the views of Russia and China with regard to internet governance. Many ASEAN nations also maintain strong state control over internet infrastructure and usage, including active censorship.[47] For example, all of the ASEAN nations signed the revised International Telecommunication Regulations promulgated at the International Telecommunication Union's 2012 World Conference on International Communications—which were boycotted by Western nations over concerns that the changes

[42] Jessica Woodall, "Australia's quiet cyber diplomacy bears fruit," *The Strategist*, Australian Strategic Policy Institute, Sept. 24, 2015, https://www.aspistrategist.org.au/australias-quiet-cyber-diplomacy-bears-fruit/
[43] "ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN," Singapore Cyber Security Agency press release, Oct. 11, 2016, https://www.csa.gov.sg/news/press-releases/asean-member-states-call-for-tighter-cybersecurity-coordination-in-asean
[44] "APCERT Conducts a Cyber Drill on an Evolving Threat and Financial Fraud," National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) press release, http://www.cert.org.cn/publish/english/55/2016/20160406131101337308175/20160406131101337308175_.html
[45] "ASEAN defense ministers stress cyber security, disaster relief in Laos," May 26, 2016, *Xinhua*, http://news.xinhuanet.com/english/2016-05/26/c_135389651.htm
[46] "ASEAN Defense Ministers Adopt PH Proposal on Cybersecurity," Department of National Defense, Republic of the Philippines press release, http://www.dndph.org/2016/asean-defense-ministers-adopt-ph-paper-on-cybersecurity
[47] Tomas Minarik, "ASEAN to Focus on Cybersecurity Capacity- and Confidence-Building in 2017," *Incyder News*, Oct. 31, 2016, https://ccdcoe.org/asean-focus-cybersecurity-capacity-and-confidence-building-2017.html

would support a national sovereignty model for internet governance.[48] Singapore, in particular, has been very active in ASEAN on that issue, dedicating $10 million to ASEAN nation capacity building between 2016-2021 at the ministerial meeting.[49] Singapore has a long tradition of censoring the press, as well as suppressing political dissent.

ASEAN and ARF, unlike some other regional organizations, do not have large support bureaucracies in place. Rather, they rely on individual nations to propose initiatives and move them forward. According to Michele Markoff, deputy coordinator for cyber issues at the U.S. State Department and one of the key negotiators of international agreements on cyber for the U.S. government, ASEAN and ARF have been "treading water" for some time in making progress toward agreed cyber norms, partly for political reasons and partly because of inertia.[50] Indeed, the OSCE on April 3, 2017 organized the first of a planned series of meetings with ARF in Korea to coordinate activities and assist the ARF in planning. Both organizations are dedicated to working together to implement the agreements made by the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security.

Despite the complications, ASEAN/ARF regional nations have been pursuing bilateral and multilateral agreements on cybersecurity, many of which are focused on improving cyber protection of communications infrastructure in the region.

OSCE

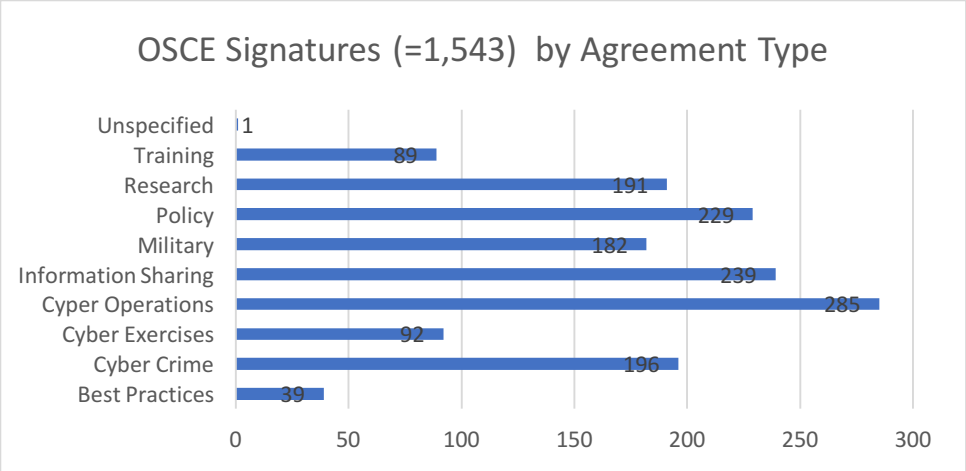
The 57-nation Organization for Security and Cooperation in Europe (OSCE) is a regional body that addresses security in a broad fashion, covering issues from human rights, economic and environmental security and democratization to arms control and confidence-building measures. Its membership comprises countries in Europe, Central Asia, and North America, including Russia and most members of the SCO (except China.) The OSCE has been working on the issue of cybersecurity since April 2012, under the auspices of an Informal Working Group (IWG) chaired by the United States.

OSCE countries account for 1,543 signatures on agreements by type amongst themselves. Cyber Operations is the largest category (285), followed by Information Sharing (239), Policy (229), Cyber Crime (196), and Research (191).

[48] "Updating International Telecommunication Regulations at WCIT 2012: Relevant for Cyber Security," *Incyder News*, Dec. 19, 2012, https://ccdcoe.org/updating-international-telecommunication-regulations-wcit-2012-relevant-cyber-security.html; Daniel Kehl and Tim Maurer, "Did the U.N. Internet Governance Summit Actually Accomplish Anything?" *Future Tense*, Dec. 14, 2012, http://www.slate.com/blogs/future_tense/2012/12/14/wcit_2012_has_ended_did_the_u_n_internet_governance_summit_accomplish_anything.html

[49] Dean Koh, "Singapore announces three broad proposals at the ASEAN Ministerial Council on Cybersecurity," *OpenGov Asia*, Oct. 11, 2016, http://www.opengovasia.com/articles/7181-enhancing-cybersecurity-in-asean-singapore-announces-three-broad-proposals-at-the-asean-ministerial-conference-on-cybersecurity

[50] Remarks at "Cyber Norms Revisited: International Cybersecurity and the Way Forward," Carnegie Endowment for International Peace, Feb. 6, 2017.



In December 2013, the IWG agreed to 11 CBMs that will be pursued by the members of the OSCE. The recommendations are broken down into three types: information sharing, mechanisms for ongoing dialogue, and capacity building. Examples include: exchanging views on perceptions of the threats to and from the use of ICTs at the national and multinational level; consultations to reduce misperceptions and tensions; setting up contact points to ensure consistent and efficient dialogue on security threats; and exchanging best practices, including those regarding effective responses to threats and incidents.[51]

A key focus of the OSCE's work has been on protection of critical infrastructure. Indeed, specific language on critical infrastructure protection was a centerpiece of a set of five additional norms agreed to by the OSCE in March 2016. In particular, CBM 15 recommended that states should work together to: "discuss opportunities and address challenges to national as well as trans-border ICT networks, upon which such critical infrastructure relies." This should include "developing, where appropriate, shared responses to common challenges including crisis-management procedures in case of widespread or transnational disruption of ICT-enabled critical infrastructure."[52]

As a follow-up, the OSCE sponsored a conference on Feb. 15, 2017—under the chairmanship of Austria—on strengthening the implementation of the OSCE CBMs on critical infrastructure.[53] "We should keep in mind that critical infrastructures are the lifelines of States, and essential assets. They are profitable businesses and indispensable for citizens. Keeping them safe is a concern all States share," said OSCE Secretary General Lamberto Zannier. "In times when

[51] "Decision No. 1106, Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communications Technologies," PC.DEC/1106, 975th Plenary Meeting, Organization for Security and Co-operation in Europe, Dec. 3, 2013, http://www.osce.org/pc/109168?download=true

[52] "Decision No. 1202, OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communications Technologies," PC.DEC/1202, 1092nd Plenary Meeting, Organization for Security and Co-operation in Europe, March 10, 2016, http://www.osce.org/pc/227281?download=true

[53] "Cyber Security for Critical Infrastructure: Strengthening Confidence Building in the OSCE," OSCE Press Release, http://www.osce.org/event/cyber-security-for-critical-infrastructure

governments are increasingly investing in cyber capabilities, enhancing cyber resilience is not only a national exercise: it is also a contribution to international peace and security."[54]

In addition, the 2016 OSCE agreement specifically addressed cooperation in response to and recovery from vulnerabilities, calling for reporting and sharing information on remediation.

The OSCE process is viewed by participants as multilayered and designed to move forward over stages. The types of CBMs agreed upon have been categorized into three groups: posturing, communications, and preparedness. Information sharing falls under posturing, and is represented by CBMs 1, 4, 7, and 9.[55] Communications are embodied in CBMs 3, 5, 11, 8, and 13.[56]

One official said another way the incremental OSCE process can be viewed is by seeing the 2013 set of CBMs as primarily transparency measures, whereas the 2016 set was focused on cooperative measures. Some OSCE members (led by the Dutch, Germans, and Austrians) hope that a third set comprised of "stability" measures will be forthcoming in the future, but that is unlikely in the next couple of years. The current focus of discussions is on implementation of the CBMs already agreed upon. For example, the OSCE is working on a method to integrate cyber crisis communications in the OSCE Communications Network set up to implement the 2011 Vienna Document designed to increase transparency and openness about military activities in the region.

Perhaps because of the low profile of the exercise, the OSCE has been able to take discussions of confidence building on cybersecurity to a surprisingly deep level. According to one expert, 52 of the 57 member states have implemented at least one of the agreed CBMs at a national level, and some members have implemented many more. CBM 8, on developing points of contact, is the one with the most successful implementation, and the OSCE Secretariat is developing a project to help less advanced states figure out who within their domestic government should be assigned as the official point of contact. This is sometimes more difficult than it sounds, due to unclear lines of authority within national governments and lack of capacity in the cyber domain. CBM 7 (sharing information on national policies/programs), CBM 1 (providing national views on national and transnational threats) and CBM 4 (sharing information on state measures to ensure an "open, interoperable, secure and reliable Internet") also have been widely embraced by member states.

When comparing the SCO and OSCE agreements, a stark difference in approach is apparent. While the SCO agreement largely seeks to shape the international political environment regarding internet control and governance, the OSCE agreement is focused on practical measures to reduce risks of conflict and improve cybersecurity across the region.

Another difference between the SCO and the OSCE processes is that the OSCE is actively seeking input from the private sector and non-governmental organizations, recognizing that buy-in from those sectors will be critical in underpinning successful adoption of the CBMs by states.

[54] "Protecting critical infrastructure from cyber attacks is crucial for international peace and security, say participants of OSCE conference in Austria," OSCE Press Release, February 16, 2017, http://www.osce.org/cio/300271
[55] Decision No. 1202, op cit
[56] Ibid

At a meeting hosted by Switzerland in November 2014 designed to support the OSCE process, Alexey Lyzhenkov, OSCE Coordinator of Activities to Address Transnational Threats, said: "While the CBMs are primarily designed for national policy-makers, their effective implementation requires the constructive engagement with non-state stakeholders."

Despite some progress in recent years, the broader disconnect between Russia (and some other Eastern European states) and the United States and other Western countries— especially as the Ukraine crisis has continued—also has affected the OSCE deliberations. One European participant in the OSCE deliberations said that recent activities by Russia, including the hacking of the U.S. Democratic National Committee, have further soured efforts at progress. Markoff, in remarks to the Carnegie Endowment on International Peace on Feb. 6, 2017, said that the U.S. government does not see pursuit of additional cyber norms as a near-term goal. Instead, the Trump administration's focus will be on "consolidating" gains so far. Other officials have echoed the U.S. sentiment that the time is not ripe for new measures, and that the central focus should be on ensuring that OSCE member states implement the current agreements and work to universalize these norms.

UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security

The issue of ICTs and security has been on the agenda of the United Nations since 1998, spurred by a Russian resolution in the First Committee, the body of the UN General Assembly that deals with international security issues. Since that time there have been four UN GGEs (under First Committee auspices) on "information security" aimed at identifying and cooperatively mitigating threats to international security emanating from use of the cybersphere. GGEs are appointed by the Secretary-General (based on national nominations) to make recommendations on emerging issues and usually are made up of 15 national representatives, with the Permanent Five members of the Security Council usually participating. Recommendations and reports require consensus. Reports are submitted to the First Committee for approval and subsequently to the UN General Assembly. If approved, these reports then take on some aspects of "soft law"—as they represent politically binding agreements that have been endorsed by the General Assembly.

The first GGE took place in 2004-2005 and did not result in a consensus report, due to two major substantive disagreements: the first regarded whether and how to characterize threats to international peace that might arise from military use of ICTs; and the second, whether discussions should include concerns regarding information content (as championed by Russia) or focus instead on protection of information infrastructure (as championed by the United States and other Western governments.)[57]

[57] "Developments in the Field of Information and Telecommunications in the Context of International Security," UNODA Fact Sheet, July 2015, UN Office of Disarmament Affairs, https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf

The second GGE (15 members), which ran in 2009-2010, resulted in an agreement on basic principles, including the need for dialogue on development of norms to reduce risks of conflict and to protect critical infrastructure, as well as a call for development of TCBMs.[58]

The third GGE (15 members), which met in 2012-2013, resulted in three types of recommendations: norms, rules, and principles of responsible behavior; TCBMs; and capacity building measures. In particular, the GGE agreed to the following:

- International law, in particular the UN Charter, is applicable to the cyber-sphere and is essential for an open, secure, peaceful, and accessible ICT environment.
- State sovereignty applies to States' conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.
- State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms.
- States must not use proxies to commit internationally wrongful acts and must ensure that their territories are not used by non-State actors for unlawful use of ICTs.
- There is a need for increased cooperation among States to address incidents that affect ICTs or critical infrastructure.[59]

The 2014-2015 GGE made substantial recommendations on norms, TCBMs, and the application of international law.[60] In particular, the 2015 GGE report emphasizes the centrality of cooperative protection of critical infrastructure, especially that which crosses national borders. It also is more specific in recommendations regarding the exchange of information on incidents, and cooperative response to/recovery from incidents. For example, the report states that:

- "States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats"; and

- "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account the due regard for sovereignty."[61]

[58] See the GGE report, A/65/201 at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/469/57/PDF/N1046957.pdf?OpenElement
[59] UNODA Fact Sheet, op cit; See GGE report, A/68/98*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement
[60] See GGE Report, A/70/174, https://disarmament-library.un.org/UNODA/Library.nsf/93a4b64e6849591d85257ddc006cbf21/49ef2dd67a02448b85257ea0006d13dd/$FILE/A%2070%20174%20GGE%20on%20Information%20&%20Telecomms%20in%20the%20field%20of%20International%20Security.pdf
[61] Ibid.

The latest GGE, which was expanded to include 25 members, began meeting in August 2015, and held its final meeting June 19-23, 2017. The June meeting, however, failed to reach a consensus. According to officials involved, the key issue of dissent at the June meeting was how to apply international law in the cybersphere, particularly the Law of Armed Conflict (LoAC) and Security Council Article 51 on self-defense. China has long voiced concern that by spelling out the applicability of LoAC and Article 51, the United Nations could be seen as sanctioning the use of cyber tools in conflict. Russia, along with a handful of non-aligned movement (NAM) states, has supported this view, also arguing that the legal issues need more time to be properly addressed.

Miguel Rodríguez, the GGE representative of Cuba, summed up these concerns in his June 23 statement:[62]

> I must register our serious concern over the pretension of some, reflected in paragraph 34 of the draft final report, to convert cyberspace into a theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs. We consider unacceptable the formulations contained in the draft, aimed to establish equivalence between the malicious use of ICTs and the concept of "armed attack", as provided for in Article 51 of the Charter, which attempts to justify the alleged applicability in this context of the right to self-defense.
>
> To establish as a precedent this dangerous reinterpretation of the norms of international law and the Charter of the United Nations would be a fatal blow to the collective security and peacekeeping architecture established in the Charter of the United Nations. The "Law of the Jungle" cannot be imposed, in which the interests of the most powerful States would always prevail to the detriment of the most vulnerable.
>
> The final draft also made reference to the supposed applicability in the context of ICT of the principles of International Humanitarian Law. We cannot accept such affirmation, since it would legitimize a scenario of war and military actions in the context of ICT.

Markoff, U.S. representative to the GGE, made the following statement at the end of the GGE meeting on June 23:

> Throughout the 2016-2017 GGE, I have sought clear and direct statements on how certain international law applies to States' use of ICTs, including international humanitarian law, international law governing States' exercise of their inherent right of self-defense, and the law of State responsibility, including countermeasures. I sought such statements in the interests of international peace and security, based on my strong conviction that the framework of international law provides States with binding standards of behavior that can help reduce the risk of conflict by creating stable expectations of how States may and may not respond to cyber incidents they face. The final draft of the report insufficiently addresses these issues. I believe it would be a troubling and potentially destabilizing signal for this GGE to release a report that does not take a clear position on the applicability of these bodies of international law to States' use of ICTs, much less fulfill the mandate given to this Group by the UN General Assembly to study *how* international legal rules and principles apply to the use of ICTs.

[62] "Declaration of Miguel Rodríguez, Representative of Cuba, at the Final Session of the Group of Governmental Experts on Developments in the Field of Information and Communications Technology in the Context of International Security," New York, June 23, 2017, https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf

> Despite years of discussion and study, some participants continue to contend that it is premature to make such a determination and, in fact, seem to want to walk back progress made in previous GGE reports. I am coming to the unfortunate conclusion that those who are unwilling to affirm the applicability of these international legal rules and principles believe their States are free to act in or through cyberspace to achieve their political ends with no limits or constraints on their actions. That is a dangerous and unsupportable view, and it is one that I unequivocally reject.
>
> During this GGE, I heard repeated assertions on the part of some participants that a discussion of certain bodies of international law, including the *jus ad bellum*, international humanitarian law, and the law of State responsibility, would be incompatible with the messages the Group should be sending regarding the peaceful settlement of disputes and conflict prevention. That is a false dichotomy that does not withstand scrutiny. A report that discusses the peaceful settlement of disputes and related concepts but omits a discussion of the lawful options States have to respond to malicious cyber activity they face would not only fail to deter States from potentially destabilizing activity, but also fail to send a stabilizing message to the broader community of States that their responses to such malicious cyber activity are constrained by international law.[63]

There also were concerns from developing nations such as Egypt, Kenya, and Indonesia about accessibility and capacity building. Another issue that was resolved is how to discuss state versus non-state malicious activities. Further, there remains contention around the issue of how states can respond to cyber attacks, including whether retaliation with non-cyber means, such as sanctions or military force, should be allowed.

Finally, there was discussion, but no agreement, about whether the United Nations should have a continuing role, and if so, what that should be. This is especially pertinent to implementation of the agreed recommendations: Is this a state responsibility, or does the United Nations have a role in, for example, developing templates for information sharing and requests for assistance? Is there a need for another GGE? How can the GGE recommendations be better socialized among UN member states, and universalized—for example, might the United Nations First Committee institute an annual review process of implementation? As an alternative, SCO members, led by Russia, have proposed opening negotiations on an International Code of Conduct for cyber activities, but this has been rejected by the United States. Cuba has gone so far as to call for the negotiation of an international legally binding instrument on applying international law in the cyber realm under the auspices of a new Working Group of the General Assembly.

Despite failure to reach consensus at the final GGE meeting, Karsten Geier, chair of the GGE and head of the cyber policy coordination staff at the German Foreign Office, noted in a speech at the Tel Aviv Cyber Week conference held June 25-29, 2017, that there were numerous areas of agreement. These include: emerging risks such as the use of cyber technologies by terrorists; capacity-building measures; and, confidence-building measures/norms, including raising awareness among senior decision-makers, conducting exercises, defining protocols for notifications about incidents, providing warning when critical infrastructure is attacked, and preventing non-state actors from conducting cyber attacks. He also noted that the group has given consent for continued work on a final report in hopes of finding some compromise.[64]

---

[63] Michele Markoff, "Explanation at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security," June 23, 2017, https://usun.state.gov/remarks/7880

[64] "UN GGE: Quo Vadis," *Geneva Digital Watch Issue 22*, June 30, https://dig.watch/DWnewsletter22

The failure of the GGE to reach consensus is a step backward for that group. It remains to be seen whether a report will be forthcoming—negotiations are continuing to seek some consensus. It is not beyond precedent that a report could be issued by the Chair that reflects areas of consensus and areas of disagreement.

In the longer term, there is the important question of how far the GGE and the OSCE norm setting processes should go to constrain destabilizing state behaviors. The Netherlands, Germany, and Switzerland had been pushing the GGE to promote the concept of creating a taboo against attacks on the backbone of the Internet (such as core data routers and the domain name system), and improving cooperative work to protect that infrastructure. This is an issue they have also raised in the OSCE process. However, that effort was not formally taken up by 2016-2017 GGE, according to Dutch officials.

Informal Fora

According to experts, informal cooperation between governments and private sector companies about vulnerabilities has improved over the past several years. Yet, difficulties remain, as witnessed by the WannaCry ransomware attacks in 2017 that led Microsoft to decry the rise of government-sponsored cyber attacks and government activities in developing/hoarding cyber exploits.

Informal fora such as conferences, workshops, and NGO/private sector-organized meetings serve as a major conduit of cybersecurity information sharing. The Dutch-funded Global Forum on Cyber Expertise is aimed at sharing technical information regarding cyber protection, and the newly formed Global Commission on Cyber Stability, headquartered in The Hague and also sponsored by the government of The Netherlands, is working on an informal basis to forward norms. The Global Conference on Cyberspace, initiated in 2011 in London and taking place biannually, is a major forum that brings together national governments, the private sector and civil society to promote practical cooperation in cyberspace, enhance capacity building, and discuss norms of responsible behavior. There have been four Global Conferences (London, Budapest, Seoul, the Hague), with the next one to be held by India in December 2017

Microsoft has developed its own proposed set of international cyber norms. In a paper released in December 2014, "International Cybersecurity Norms: Reducing Conflict in an Internet Dependent World," Microsoft laid out a need for two types of norms:

- "Norms for improving defenses, which can reduce risk by providing a foundation for national cybersecurity capacity and for domestic, regional, and international organizational structures and approaches that increase understanding between states.
- Norms for limiting conflict or offensive operations, which will serve to reduce conflict, avoid escalations, and limit the potential for catastrophic impacts in, through, or even to cyberspace."[65]

[65] Angela McKay, Jan Neutze, Paul Nicholas, Kevin Sullivan, "International Cybersecurity Norms: Reducing conflict in an Internet dependent world," Microsoft, December 2014, file:///Users/theresahitchens/Downloads/International_Cybersecurity_%20Norms.pdf

The company has vocally expressed concerns about the growth in state-sponsored offensive cyber operations. The paper explains:

> However, offensive cyber operations can result in unintended consequences. Given the interconnected nature of cyberspace and the speed and nature of cyber attacks, the effects of offensive operations might be very difficult to predict and/or limit, and they could cascade to affect operations beyond the intended targets, including critical functions in the energy, communications, banking, chemical, or transportation sectors, among others. In other instances, an offensive cyber operation gone wrong could disrupt the global Internet or corrupt data at a scale that impedes key functions of the global economy. Unintended consequences of this scale could very easily escalate hostilities from the keyboard to kinetics, in the absence of normative limits on such behaviors.

Microsoft therefore proposed six norms of behavior:

- "Norm 1: States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.
- Norm 2: States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
- Norm 3: States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.
- Norm 4: States should commit to nonproliferation activities related to cyber weapons.
- Norm 5: States should limit their engagement in cyber offensive operations to avoid creating a mass event.
- Norm 6: States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace."

Microsoft is cosponsoring the Global Commission on Cyber Stability and has been heavily involved in promoting its approach. However, it has not been successful in rallying other major internet companies to its cause. There remains suspicion in corporate circles, as well as within developing nations, about the company's motivations.

Conclusions

This survey of international cyber information sharing agreements produced a number of key findings:

- Extensive signature of agreements and associated commentary shows widespread accord in principle that information sharing is necessary, but it is unclear how much and what type of information sharing occurs in practice.
- The U,S. U.K., the Netherlands, Spain, and India have signed the most agreements.
- Few agreement texts are public, and those that are, often use vague language.
- Many government agreements are at the agency level, i.e. between CERTs.
- Many agreements are found only via public statements and press reports.

- Much information sharing takes place informally, such as during IGO cyber exercises and at regularized fora such as Track 1.5 conferences.
- Many countries have signed regional accords but few bilateral ones.
- Much activity is aimed at awareness raising and bolstering national capacities, especially for countries with less-developed ICT infrastructure.
- National security concerns continue to dominate, according to officials involved, and thus mitigate against effective collective measures.
- Even among NATO members with collective assets, barriers remain to cooperation (including pursuit of offensive tools), according to experts.
- China is more active than Russia in sharing arrangements.
- Russian sharing agreements are largely political, to gather support for the concept of "information security" and strong national control of content.
- Russia-China technical cooperation is largely one-way—with China helping Russia to build a centralized Internet system similar to the Chinese Great Firewall.

While states at the political level agree that there is a need for cooperation to protect the cybersphere, as often in multilateral diplomacy, the devil is in the details. At a workshop held by CISSM in June 2017, experts listed a number of reasons that states might share, or not share information about cyber threats and incidents. These were as follows:

<u>Reasons to share information (bilaterally or globally)</u>

- Mutual benefit to sharing information because everyone will be damaged in the event of a cyber incident
- Faster response
- Prevention (vulnerability information, remedies, threat actors)
- Detection (attribution, motives, methods)
- Capacity building to prepare for the future
- Relationship building (trust, confidence in cyber sphere, as a vehicle for other relationships—military, economic, political)
- Identify emerging threats and trends
- Reassurance (self-restraint, clear self of blame)

<u>Reasons not to share information: (national or alliance)</u>

- Need time to fix the vulnerability before others know it
- Leveraging competitive advantage (keep vulnerabilities secret—to sell a product or not to lose customers, protect reputation, speed of remediation relative to competitor)
- Not trust the other country (they could use it on someone else or not use it appropriately)

- Defense of sources and methods
- Offensive use (intel/sources and methods, cyber attack)
- No incentive: do not understand the value of sharing
- Lack the capability (internally to protect "equities" and not let others know unsavory stuff you are doing), or internationally (no POC, methodology)
- Withhold information as leverage, bargaining chip over another country or let them suffer the consequences

Given the complexity of the problems faced in improving cybersecurity—problems that require different types of actions and different legal/diplomatic tools to resolve—it is unrealistic to expect rapid progress towards norm setting and conflict prevention/resolution. On the other hand, there is movement among states to find ways to cooperate on network and critical infrastructure protection, build technical capacity, and develop best practices that can be shared. CERT-to-CERT cooperation is broadly moving toward the routine, but is sometimes hampered by political considerations in information sharing. More in-depth cooperation on issues such as incident reporting and response remains confined to political allies, mostly in Western states where use of the cybersphere is more advanced and governments are more likeminded.

Cyber sharing remains challenged by political differences toward freedom of information and individual privacy (where gaps exist even among Western nations), perceived national security concerns, secrecy, and even different models of economic development and the role of private industry. Another issue at hand is the technology gap. Developing countries continue to voice concern about the fact that their populations by and large rely on older versions of ICT technology, requiring different approaches to cybersecurity. For example, in developing countries such as Kenya, many people access the internet on a price per gigabyte basis, which means many skip downloading automatic patches to software because doing so eats up all their available bandwidth. According to one Kenyan official, developing countries are more interested in ensuring sustainability of the technology they already have invested in rather than seeking simply to replace it.

The growing number of cybersharing agreements over the last five years points to growing concerns about the safety of the domain, as the economic value of cyber activity increases. However, the lack of public information about the details of these agreements—and the vagueness of many that are in the public domain—makes it difficult to assess the impact of these agreements on either improving international cybersecurity or successful norm setting.

Both current norm setting activity and cybersharing activity seems to be happening at a political level, but not necessarily at a deeply practical level beyond efforts to improve national technical capabilities. The exception to this, according to diplomats involved in multilateral and regional discussions, is at the CERT-to-CERT level, where there are almost daily interactions, and clear processes. At the state-to-state level, however, information sharing is more difficult to implement. For example, while states have agreed to a norm to prevent and restrain attacks on critical infrastructure, Eviatar Matania, head of Israel's National Cyber Bureau, recently raised a key problem: there is no agreed definition of critical infrastructure. "The norm of 'do not attack

critical infrastructures' sounds great, but can you define for me what critical infrastructures are?" he said at a September 2016 cybersecurity conference in Washington, D.C. "The definition in every nation is different. Some will define everything as critical."[66]

Given that increased transparency is one goal of the ongoing multilateral norm-setting processes both at the United Nations and within regional organizations, the paucity of detailed public domain information about cybersharing activities also reflects tension within and among states. The tension arises from understanding that cooperation is necessary to improve national cybersecurity for all and the internal pressures for secrecy and government control of cyber networks deemed critical to national security. That said, if the focus of multilateral efforts in the coming years is to be on forwarding implementation of the norms and TCBMs agreed so far, further research should be able to chart with more fidelity actual information sharing practices.

Next Steps

This initial research has discerned some interesting dynamics on the structure of current information sharing agreements. Future work will more fully explore the decision processes and actions associated with implementation, with particular attention to the underlying factors affecting when information on a range of cyber events is likely to be passed from one party to another. The goal is to improve implementation of current agreements by states and identify where new or more specific agreements could be helpful.

In particular, CISSM plans to concentrate on the further development of a framework for cybersecurity needs assessment that will assist policy-makers in prioritizing what types of cyber information sharing for prevention and incident response would be most valuable, and help them think through benefits, costs, and risks associated with sharing different types of cyber information with different kinds of countries under various scenarios.

CISSM also intends to hold cybersecurity information sharing table-top exercises involving policy-makers both at a national and multinational level. The project held a prototype exercise on June 5-6, 2017 involving 11 participants (including non-U.S.) that looked at information sharing prior to an incident, after an isolated attack, and after a campaign of attacks involving more than one state. As expected, the exercise showed greater willingness among participants to share information in a post-attack environment, even though preventive sharing could have been more beneficial. Participants also were more willing to share information regarding cyber criminals than regarding terrorist organizations, or other states. Further, during the exercises, it became clear that the more one actor shared its information, the more other actors were willing to reciprocate. Finally, another insight was that even a smaller, less advanced state is often privy to information that is not held by larger, more sophisticated states due to geopolitical realities. The project team intends to use the lessons learned from the pilot exercise to refine the scenarios and tailor the exercise to different audiences.

[66] Joe Uchill, "Israel cyber head: US-backed cyber norms too broad," *The Hill*, Sept. 13, 2016, http://thehill.com/policy/cybersecurity/295651-israel-cyber-head-us-supported-cyber-norms-too-broad

International Cybersecurity Information Sharing Agreements

ANNEX 1 – Methodology

The researchers conducted open source, web-based research in English to survey, review, and catalogue cybersecurity information sharing agreements at the bilateral, regional, and international levels. The main sources of data were government documents, press releases, articles, policy reports, newspaper articles, and email correspondence with experts. Each country and regional bloc features an extensive bibliography consisting of these sources. Additional information was collected through contacting government officials when possible, in cases where detailed information on an agreement was not available on the web.

The researchers then created a database using a Microsoft Access user interface (UI) macro. The database is designed as a quantitative tool to generate data on the numbers and types of cybersecurity information sharing agreements. After several iterations on the design, the database features tables for agreements, list of agreements with details, and reference tables for the country master list and agreement types, i.e. best practices, cyber crime, cyber exercises, cyber operations, information sharing, military, policy, research, and training. Broad cooperation agreements are listed under "policy." The database not only lists agreements but also displays data on various dimensions across country levels of activity, regional blocs, and types of cybersecurity cooperation. It can also be used to create a timeline of agreements.

The database uses a standardized language, e.g. CERT (country name), MoU between (country name) and (country name). For each agreement, the database lists the name, the category, date of signature, expiration date, the signatories, links to the agreement text where available, and a summary of the agreement's main points. In cases of multilateral treaties and conventions, all countries that are signatories are listed. The database also features the involved entities in each agreement, i.e. CERT-to-CERT, government-to-government, industry-to-industry, agency-to-agency, and variations. In some instances, NGOs and universities are included.

In terms of data entry criteria, both formal and informal, institutionalized agreements are listed as long as they are regular and systematically pursued to share information on cybersecurity. Accounting for the differences in terminology among countries, agreements on information and communications technology (ICT) are also included. Countries' membership to cyber-related organizations, however, are not included if they do not pertain to an agreement. Similarly ad hoc meetings, events, initiatives, networks, and multinational research projects are not listed unless they are part of an agreement.

At a macro-level, the research documented 196 agreements involving 116 countries. In total, these agreements involve 2,349 signatures when broken down by type.

ANNEX 2 – Informal Translation of Russia-China on Cooperation in the Field of International Information Security

GOVERNMENT OF THE RUSSIAN FEDERATION
Deposited on
April 30, 2015 № 788-r
MOSCOW

On signing the Agreement between the Russian Federation and the Government of the People's Republic of China on cooperation in the field of international information security

Approve in accordance with paragraph 1 of Article 11 of the Federal law "On international treaties of the Russian Federation" presented by Russian Ministry of Foreign Affairs and coordinated with other interested federal executive bodies and tentatively agreed with the Chinese side a draft agreement between the Russian Federation and the Government of the Peoples Republic of China on cooperation in the field of international information security (attached).

Instruct Russian Foreign Ministry to hold talks with the Chinese side and on reaching the agreement - sign it on behalf of the Government of Russian Federation, allowing to make changes in the attached project that do not represent a matter of principle.

The Government of the Russian Federation and the Government of the People's Republic of China, hereinafter referred to as by the Parties, in accordance with the provisions of the Treaty of Good-Neighborliness, Friendship and Cooperation between the Russian Federation and the People's Republic of China on July 16, 2001,

Noting substantial progress in the development and introduction of new information and communication technologies, forming the global information space,

Underlining a great importance to the role of ICT in promoting social and economic development for the benefit of all humanity and the maintenance of international peace, security and stability,

Expressing concern for the threats related to the use of such technologies in the civilian and military purposes not inconsistent with the objectives of international peace, security and stability, with the goal of undermining the sovereignty and security of states and interfering in their internal affairs and violating the privacy of citizens, destabilizing the political and socio-economic environment, stirring up national and religious hatred,

Attaching great importance to international information security as to one of the key elements of the system of international security,

Reaffirming that the sovereignty and international norms and principles, arising from state sovereignty, apply to the conduct of states in the framework of the activities,

Related to the usage of information and communication technologies, and the jurisdiction of states over the information infrastructure on their territory, and that the state has the sovereign right to define and implement public policy on matters relating to information and telecommunications "Internet" network, including security provision,

Emphasizing the collaboration within the framework of the Shanghai Cooperation Organization,

Convinced that the further deepening of trust and development of cooperation between the Parties in the field of information and communication technologies are an imperative and in serve their best interest,

Taking into account the important role of information security in ensuring the rights and fundamental freedoms of men and citizen,

Attaching great importance to the balance between security and human rights in the field of information and communication technologies,

In order to prevent threats to international information security and ensure information security interests of the Parties in order to create an international information environment, which is characterized by peace and cooperation,

Trying to form a multilateral, transparent and democratic regulation of international information and telecommunications network "Internet" with a view to the internationalization of management information and telecommunications network "Internet" and to ensure equal rights of states to participate in the process of the system's control, including democratic management of basic resources of information and telecommunication network "Internet "and their equitable distribution,

Desiring to create a legal and organizational framework for cooperation between the Parties in the field of international information security,

Have agreed as follows:

Article 1. Main definitions.

Article 2. The main threats in the field of international information security.

Article 3. Key areas of cooperation.
In view of the major threats referred to in Article 2 of this Agreement, authorized representatives of the Parties and the competent authorities of the Parties, which are determined in accordance with Article 5 of this Agreement, shall cooperate in the field of international information security in the following areas:

1) definition, coordination and implementation of the necessary cooperation in the field of international information security;

2) establishment of communication channels and contacts in order to jointly respond to threats in the field of international information security;

3) cooperation in developing and promoting standards international law in order to ensure national and international information security;

4) joint response to threats in the field of international information security as defined in Article 2 of this Agreement;

5) information exchange and law enforcement cooperation with a view to the investigation of cases involving the use of information and communication technologies for terrorist and criminal purposes;

6) development and implementation of the necessary joint confidence-building measures that contribute to ensuring international information security;

7) cooperation between the competent authorities of the Parties in the area of security provision to the critical information infrastructure of the Parties, technology exchange and cooperation between the competent authorities of the Parties in the field of Computer Emergency Response;

8) information exchange on the Parties legislation on issues of information security;

9) promotion of the improvement of the international legal framework and practical mechanisms for cooperation between the Parties in ensuring international information security;

10) creation of conditions for cooperation of the competent authorities of the Parties in order to implement this Agreement;

11) the deepening of cooperation and coordination of activities of the Parties on issues of international information security within the framework of international organizations and forums (including the United Nations, the International Telecommunication Union, the International Organization for Standardization, the Shanghai Cooperation Organization, BRICS countries, the Regional Security Forum of ASEAN and others);

12) the promotion of research in the field of international information security, joint research projects;

13) joint training, exchange of students and teachers from specialized higher education institutions;

14) holding working meetings, conferences, seminars and other forums of the delegates and experts representing the Parties in the field of international information security;

15) establishment of a mechanism for cooperation between the competent authorities of the Parties with a view to exchanging and sharing of information on existing and potential risks, threats and vulnerabilities in the area of information security - their identification, assessment, research, mutual exchange of information about them and prevention of their occurrence.

2. The Parties or the competent authorities of the Parties may, by mutual agreement to define other areas of cooperation.

Article 4. General principles of cooperation.

Article 5. Basic forms and mechanisms of cooperation.

1. Practical cooperation in specific areas of cooperation under this Agreement, the Parties may exercise through the competent authorities of the Parties responsible for the implementation of this Agreement. Within 60 days from the date of entry into force of this Agreement, the Parties will exchange via diplomatic channels the data on competent authorities of the Parties responsible for the implementation of this Agreement.

2. In order to establish the legal and institutional framework for cooperation in specific areas of the competent authorities of the Parties may conclude appropriate agreements of interdepartmental character.

3. The procedure of exchange defined in subparagraph 15 of paragraph 1 of Article 3 of this Agreement, as well as used message formats and the means of protection of transmitted information are determined by corresponding agreements between the competent authorities of the Parties.

4. In order to review the implementation of this Agreement, the exchange of information, analysis and the joint assessment of emerging threats to information security, as well as the definition, harmonization and coordination of a joint response to such threats Parties shall hold consultations on a regular basis, and authorized representatives of the competent authorities of the Parties. Consultations are carried out by agreement of the Parties, usually 2 times a year, alternately in the Russian Federation and the People's Republic of China. Each of the Parties may initiate further consultation, offering time and place of the meeting and the agenda.

Article 6. Data protection.

Article 7. Financing.

Article 8. Relation to other international agreements.

This Agreement does not affect the rights and obligations of the Parties under other international treaties to which it is a member, nor it is directed against any third country.

Article 9. Settlement of disputes.

Article 10. Final provisions.

1. This Agreement is concluded for an indefinite period and shall enter into force on the 30th day following the date of receipt through diplomatic channels of the last written notification on fulfillment by the Parties of internal procedures necessary for its entry into force.

2. The parties may make changes to this Agreement, which by mutual agreement of the Parties are executed as a separate protocol.
3. This Agreement may be terminated at the expiration of 90 days from receipt of one of the Parties through diplomatic channels, written notice of the other party of its intention to terminate this Agreement.
4. In the event of termination of this Agreement, the Parties shall take measures to fully implement the obligations to protect information and ensure compliance with previously agreed joint activities, projects and other activities carried out under this Agreement and not completed at the time of termination of this Agreement.

Done at, "" 2015, in two copies, in Russian and Chinese languages, both texts being equally authentic.

ANNEX 3 – Russian Original, Russia-China on Cooperation in the Field of International Information Security

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

Р А С П О Р Я Ж Е Н И Е

от 30 апреля 2015 г. № 788-р

МОСКВА

О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности

В соответствии с пунктом 1 статьи 11 Федерального закона "О международных договорах Российской Федерации" одобрить представленный МИДом России согласованный с другими заинтересованными федеральными органами исполнительной власти и предварительно проработанный с Китайской Стороной проект Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности (прилагается).

Поручить МИДу России провести переговоры с Китайской Стороной и по достижении договоренности подписать от имени Правительства Российской Федерации указанное Соглашение, разрешив вносить в прилагаемый проект изменения, не имеющие принципиального характера.

Председатель Правительства
Российской Федерации Д.Медведев

Проект

С О Г Л А Ш Е Н И Е

между Правительством Российской Федерацией
и Правительством Китайской Народной Республики
о сотрудничестве в области обеспечения международной
информационной безопасности

Правительство Российской Федерации и Правительство Китайской Народной Республики, далее именуемые Сторонами,

руководствуясь положениями Договора о добрососедстве, дружбе и сотрудничестве между Российской Федерацией и Китайской Народной Республикой от 16 июля 2001 года,

отмечая значительный прогресс в развитии и внедрении новейших информационно-коммуникационных технологий, формирующих глобальное информационное пространство,

придавая важное значение роли информационно-коммуникационных технологий в содействии социально-экономическому развитию на благо всего человечества и поддержании международного мира, безопасности и стабильности,

выражая озабоченность угрозами, связанными с возможностями использования таких технологий в гражданской и военной сферах в целях, не совместимых с задачами обеспечения международного мира, безопасности и стабильности, для подрыва суверенитета и безопасности государств и вмешательства в их внутренние дела, нарушения неприкосновенности частной жизни граждан, дестабилизации внутриполитической и социально-экономической обстановки, разжигания межнациональной и межконфессиональной вражды,

придавая важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности,

подтверждая то, что государственный суверенитет и международные нормы и принципы, вытекающие из государственного суверенитета,

распространяются на поведение государств в рамках деятельности, связанной с использованием информационно-коммуникационных технологий, и юрисдикцию государств над информационной

инфраструктурой на их территории, а также то, что государство имеет суверенное право определять и проводить государственную политику по вопросам, связанным с информационно-телекоммуникационной сетью "Интернет", включая обеспечение безопасности,

придавая особое значение совместной работе в рамках Шанхайской организации сотрудничества,

будучи убежденными в том, что дальнейшее углубление доверия и развитие взаимодействия Сторон в области использования информационно-коммуникационных технологий являются настоятельной необходимостью и отвечают их интересам,

принимая во внимание важную роль информационной безопасности в обеспечении прав и основных свобод человека и гражданина,

придавая важное значение балансу между обеспечением безопасности и соблюдением прав человека в области использования информационно-коммуникационных технологий,

стремясь предотвращать угрозы международной информационной безопасности, обеспечить интересы информационной безопасности Сторон в целях формирования международной информационной среды, для которой характерны мир и сотрудничество,

стремясь формировать многостороннюю, демократическую и прозрачную международную систему управления информационно-телекоммуникационной сетью "Интернет" в целях интернационализации управления информационно-телекоммуникационной сетью "Интернет" и обеспечения равных прав государств на участие в этом процессе, включая демократическое управление основными ресурсами информационно-телекоммуникационной сети "Интернет" и их справедливое распределение,

желая создать правовые и организационные основы сотрудничества Сторон в области обеспечения международной информационной безопасности,

согласились о нижеследующем:

Статья 1

Основные понятия

Для целей взаимодействия Сторон в ходе выполнения настоящего Соглашения используются основные понятия, перечень которых приведен в приложении, являющемся неотъемлемой частью настоящего

3

Соглашения. Указанное приложение может по мере необходимости дополняться, уточняться и обновляться по согласованию Сторон.

Статья 2
Основные угрозы в области обеспечения
международной информационной безопасности

При осуществлении сотрудничества в соответствии с настоящим Соглашением Стороны исходят из того, что основными угрозами международной информационной безопасности являются использование информационно-коммуникационных технологий:

1) для осуществления актов агрессии, направленных на нарушение суверенитета, безопасности, территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

2) для нанесения экономического и другого ущерба, в том числе путем оказания деструктивного воздействия на объекты информационной инфраструктуры;

3) в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

4) для совершения правонарушений и преступлений, в том числе связанных с неправомерным доступом к компьютерной информации;

5) для вмешательства во внутренние дела государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей и теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию и нестабильности, а также для дестабилизации внутриполитической и социально-экономической обстановки, нарушения управления государством;

6) для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Статья 3

Основные направления сотрудничества

1. С учетом основных угроз, указанных в статье 2 настоящего Соглашения, Стороны, уполномоченные представители и компетентные органы государств Сторон, которые определяются в соответствии со

статьей 5 настоящего Соглашения, осуществляют сотрудничество в области обеспечения международной информационной безопасности по следующим основным направлениям:

1) определение, согласование и осуществление необходимого сотрудничества в области обеспечения международной информационной безопасности;

2) создание каналов связи и контактов в целях совместного реагирования на угрозы в сфере международной информационной безопасности;

3) взаимодействие в разработке и продвижении норм международного права в целях обеспечения национальной и международной информационной безопасности;

4) совместное реагирование на угрозы в области обеспечения международной информационной безопасности, указанные в статье 2 настоящего Соглашения;

5) обмен информацией и сотрудничество в правоохранительной области в целях расследования дел, связанных с использованием информационно-коммуникационных технологий в террористических и криминальных целях;

6) разработка и осуществление необходимых совместных мер доверия, способствующих обеспечению международной информационной безопасности;

7) сотрудничество между компетентными органами государств Сторон в области обеспечения безопасности критической информационной инфраструктуры государств Сторон, обмен технологиями и сотрудничество между уполномоченными органами государств Сторон в области реагирования на компьютерные инциденты;

8) обмен информацией о законодательстве государств Сторон по вопросам обеспечения информационной безопасности;

9) содействие совершенствованию международно-правовой базы и практических механизмов сотрудничества Сторон в обеспечении международной информационной безопасности;

10) создание условий для взаимодействия компетентных органов государств Сторон в целях реализации настоящего Соглашения;

11) углубление сотрудничества и координации деятельности государств Сторон по проблемам обеспечения международной информационной безопасности в рамках международных организаций и форумов (включая Организацию Объединенных Наций, Международный

союз электросвязи, Международную организацию по стандартизации, Шанхайскую организацию сотрудничества, страны БРИКС, Региональный форум Ассоциации государств Юго-Восточной Азии по безопасности и другие);

12) содействие научным исследованиям в области обеспечения международной информационной безопасности, проведение совместных научно-исследовательских работ;

13) совместная подготовка специалистов, обмен студентами, аспирантами и преподавателями профильных высших учебных заведений;

14) проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов государств Сторон в сфере международной информационной безопасности;

15) создание механизма сотрудничества между уполномоченными органами государств Сторон в целях обмена информацией и совместного использования информации о существующих и потенциальных рисках, угрозах и уязвимостях в области информационной безопасности, их выявления, оценки, изучения, взаимного информирования о них, а также предупреждения их возникновения.

2. Стороны или компетентные органы государств Сторон могут по взаимной договоренности определять другие направления сотрудничества.

Статья 4

Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество в области обеспечения международной информационной безопасности в рамках настоящего Соглашения таким образом, чтобы такое сотрудничество способствовало социальному и экономическому развитию, было совместимо с задачами поддержания международного мира, безопасности и стабильности и соответствовало общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы и угрозы силой, невмешательства во внутренние дела,

уважения прав и основных свобод человека, а также принципам двустороннего сотрудничества и невмешательства в информационные ресурсы государств Сторон.

2. Деятельность Сторон в рамках настоящего Соглашения должна быть совместимой с правом каждой Стороны искать, получать и распространять информацию с учетом того, что такое право может быть

ограничено законодательством государств Сторон в целях обеспечения национальной безопасности.

3. Каждая Сторона имеет равное право на защиту информационных ресурсов своего государства от неправомерного использования и несанкционированного вмешательства, в том числе от компьютерных атак на них.

Каждая Сторона не осуществляет по отношению к другой Стороне подобных действий и оказывает содействие другой Стороне в реализации указанного права.

Статья 5

Основные формы и механизмы сотрудничества

1. Практическое взаимодействие по конкретным направлениям сотрудничества, предусмотренным настоящим Соглашением, Стороны могут осуществлять по линии компетентных органов государств Сторон, ответственных за реализацию настоящего Соглашения. В течение 60 дней со дня вступления настоящего Соглашения в силу Стороны обменяются по дипломатическим каналам данными о компетентных органах государств Сторон, ответственных за реализацию настоящего Соглашения.

2. В целях создания правовых и организационных основ сотрудничества по конкретным направлениям компетентные органы государств Сторон могут заключать соответствующие договоры межведомственного характера.

3. Порядок осуществления обмена, определенного подпунктом 15 пункта 1 статьи 3 настоящего Соглашения, а также применяемые для этого форматы сообщений и средства защиты передаваемой информации определяются соответствующими соглашениями между компетентными органами государств Сторон.

4. В целях рассмотрения хода реализации настоящего Соглашения, обмена информацией, анализа и совместной оценки возникающих угроз информационной безопасности, а также определения, согласования и

координации совместных мер реагирования на такие угрозы Стороны проводят на регулярной основе консультации уполномоченных представителей и компетентных органов государств Сторон. Консультации проводятся по согласованию Сторон, как правило, 2 раза в год попеременно в Российской Федерации и Китайской Народной Республике. Каждая из Сторон может инициировать проведение дополнительных

консультаций, предлагая время и место их проведения, а также повестку дня.

Статья 6
Защита информации

1. Стороны обеспечивают надлежащую защиту передаваемой или создаваемой в ходе сотрудничества в рамках настоящего Соглашения информации, доступ к которой и распространение которой ограничены в соответствии с законодательством государств Сторон. Защита такой информации осуществляется в соответствии с законодательством и (или) соответствующими нормативными правовыми актами получающей Стороны. Такая информация не раскрывается, не передается без письменного согласия Стороны, являющейся источником этой информации, и должным образом обозначается в соответствии с законодательством государств Сторон.
2. Защита государственной тайны Российской Федерации и (или) охрана государственной тайны Китайской Народной Республики в ходе сотрудничества в рамках настоящего Соглашения осуществляются в соответствии с Соглашением между Правительством Российской Федерации и Правительством Китайской Народной Республики о взаимном обеспечении защиты и сохранности секретной информации от 24 мая 2000 года, а также законодательством и (или) соответствующими нормативными правовыми актами государств Сторон.

Статья 7
Финансирование

1. Стороны самостоятельно несут расходы по участию их представителей и экспертов в соответствующих мероприятиях по исполнению настоящего Соглашения.
2. В отношении прочих расходов, связанных с исполнением

настоящего Соглашения, Стороны в каждом отдельном случае могут согласовывать иной порядок финансирования в соответствии с законодательством государств Сторон.

8

Статья 8

Отношение к другим международным договорам

Настоящее Соглашение не затрагивает прав и обязательств каждой из Сторон по другим международным договорам, участником которых является ее государство, и не направлено против какого-либо третьего государства.

Статья 9

Разрешение споров

Стороны решают спорные вопросы, которые могут возникнуть в связи с толкованием или применением положений настоящего Соглашения, путем консультаций и переговоров между компетентными органами государств Сторон и в случае необходимости по дипломатическим каналам.

Статья 10

Заключительные положения

1. Настоящее Соглашение заключается на неопределенный срок и вступает в силу на 30-й день со дня получения по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу.
2. Стороны могут вносить в настоящее Соглашение изменения, которые по взаимному согласию Сторон оформляются отдельным протоколом.
3. Действие настоящего Соглашения может быть прекращено по истечении 90 дней со дня получения одной из Сторон по дипломатическим каналам письменного уведомления другой Стороны о ее намерении прекратить действие настоящего Соглашения.

4. В случае прекращения действия настоящего Соглашения Стороны принимают меры для полного выполнения обязательств по защите информации, а также обеспечивают выполнение ранее согласованных совместных работ, проектов и иных мероприятий, осуществляемых в рамках настоящего Соглашения и не завершенных к моменту прекращения действия настоящего Соглашения.

9

Совершено в г. " " 2015 г. в двух экземплярах, на русском и китайском языках, причем оба текста имеют одинаковую силу.

За Правительство
Китайской Народной Республики

За Правительство
Российской Федерации

Annex 4: Agreement among the Governments of the Shanghai Cooperation Organization (SCO) Member States on Cooperation in the Field of Ensuring International Information Security (Yekaterinburg, 16 June 2009), Russian Original

СОГЛАШЕНИЕ
МЕЖДУ ПРАВИТЕЛЬСТВАМИ ГОСУДАРСТВ—ЧЛЕНОВ
ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА
О СОТРУДНИЧЕСТВЕ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ
МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Екатеринбург, 16 июня 2009 года

(Вступило в силу с 5 января 2012 года)

Правительства государств — членов Шанхайской организации сотрудничества, далее именуемые «Стороны»,
отмечая значительный прогресс в развитии и внедрении новейших информационно-коммуникационных технологий и средств, формирующих глобальное информационное пространство,
выражая озабоченность угрозами, связанными с возможностями использования таких технологий и средств в целях, не совместимых с задачами обеспечения международной безопасности и стабильности, как в гражданской, так и в военной сферах,
придавая важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности,
будучи убежденными в том, что дальнейшее углубление доверия и развитие взаимодействия Сторон в вопросах обеспечения международной информационной безопасности являются настоятельной необходимостью и отвечают их интересам,
принимая во внимание важную роль информационной безопасности в обеспечении прав и основных свобод человека и гражданина,
учитывая резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»,
стремясь ограничить угрозы международной информационной безопасности, обеспечить интересы информационной безопасности Сторон и создать международную информационную среду, для которой характерны мир, сотрудничество и гармония,
желая создать правовые и организационные основы сотрудничества

Сторон в области обеспечения международной информационной безопасности,
согласились о нижеследующем:

Статья 1

Основные понятия

Для целей взаимодействия Сторон в ходе выполнения настоящего Соглашения используются основные понятия, перечень которых приведен в Приложении 1 («Перечень основных понятий в области международной

информационной безопасности»), являющемся неотъемлемой частью настоящего Соглашения.

Приложение 1 может по мере необходимости дополняться, уточняться и обновляться по согласованию Сторон.

Статья 2

Основные угрозы в области обеспечения международной информационной безопасности

Реализуя сотрудничество в соответствии с настоящим Соглашением, Стороны исходят из наличия следующих основных угроз в области обеспечения международной информационной безопасности:

1) разработка и применение информационного оружия, подготовка и ведение информационной войны;

2) информационный терроризм;

3) информационная преступность;

4) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств;

5) распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств;

6) угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

Согласованное понимание Сторонами существа перечисленных в настоящей статье основных угроз приведено в Приложении 2 («Перечень основных видов угроз в области международной информационной безопасности, их источников и признаков»), являющемся неотъемлемой частью настоящего Соглашения.

Приложение 2 может по мере необходимости дополняться, уточняться и обновляться по согласованию Сторон.

Статья 3

Основные направления сотрудничества

С учетом угроз, указанных в статье 2 настоящего Соглашения, Стороны, их уполномоченные представители, а также компетентные органы государств Сторон, которые определяются в соответствии со статьей 5 настоящего Соглашения, осуществляют сотрудничество в области обеспечения международной информационной безопасности по следующим основным направлениям:

1) определение, согласование и осуществление необходимых

совместных мер в области обеспечения международной информационной безопасности;

2) создание системы мониторинга и совместного реагирования на возникающие в этой области угрозы;

3) выработка совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия, создающего угрозы обороноспособности, национальной и общественной безопасности;
4) противодействие угрозам использования информационно-коммуникационных технологий в террористических целях;
5) противодействие информационной преступности;
6) проведение необходимых для целей настоящего Соглашения экспертиз, исследований и оценок в области обеспечения информационной безопасности;
7) содействие обеспечению безопасного, стабильного функционирования и интернационализации управления глобальной сетью Интернет;
8) обеспечение информационной безопасности критически важных структур государств Сторон;
9) разработка и осуществление совместных мер доверия, способствующих обеспечению международной информационной безопасности;
10) разработка и осуществление согласованной политики и организационно-технических процедур по реализации возможностей использования электронной цифровой подписи и защиты информации при трансграничном информационном обмене;
11) обмен информацией о законодательстве государств Сторон по вопросам обеспечения информационной безопасности;
12) совершенствование международно-правовой базы и практических механизмов сотрудничества Сторон в обеспечении международной информационной безопасности;
13) создание условий для взаимодействия компетентных органов государств Сторон в целях реализации настоящего Соглашения;
14) взаимодействие в рамках международных организаций и форумов по проблемам обеспечения международной информационной безопасности;
15) обмен опытом, подготовка специалистов, проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов Сторон в области информационной безопасности;
16) обмен информацией по вопросам, связанным с осуществлением сотрудничества по перечисленным в настоящей статье основным направлениям.
Стороны или компетентные органы государств Сторон могут по взаимной договоренности определять другие направления сотрудничества.

Статья 4

Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество и свою деятельность в международном информационном пространстве в рамках настоящего Соглашения таким образом, чтобы такая деятельность способствовала социальному и экономическому развитию и была совместимой с задачами поддержания международной безопасности и стабильности, соответствовала общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека, а также принципам регионального сотрудничества и невмешательства в информационные ресурсы государств Сторон.

2. Деятельность Сторон в рамках настоящего Соглашения должна быть совместимой с правом каждой Стороны искать, получать и распространять информацию с учетом того, что такое право может быть ограничено законодательством в целях защиты интересов национальной и общественной безопасности.

3. Каждая Сторона имеет равное право на защиту информационных ресурсов и критически важных структур своего государства от неправомерного использования и несанкционированного вмешательства, в том числе от информационных атак на них.

Каждая Сторона не проводит по отношению к другой Стороне подобных действий и оказывает содействие другим Сторонам в реализации вышеуказанного права.

Статья 5

Основные формы и механизмы сотрудничества

1. В течение шестидесяти дней с даты вступления настоящего Соглашения в силу Стороны обменяются через депозитария данными о компетентных органах государств Сторон, ответственных за реализацию настоящего Соглашения, и каналах прямого обмена информацией по конкретным направлениям сотрудничества.

2. С целью рассмотрения хода выполнения настоящего Соглашения, обмена информацией, анализа и совместной оценки возникающих угроз информационной безопасности, а также определения, согласования и координации совместных мер реагирования на такие угрозы, Стороны проводят на регулярной основе консультации уполномоченных представителей Сторон и компетентных органов государств Сторон (далее —

консультации).

Очередные консультации проводятся по согласованию Сторон, как правило, один раз в полугодие в Секретариате Шанхайской организации сотрудничества или на территории государства одной из Сторон по ее приглашению.

Любая из Сторон может инициировать проведение внеочередных консультаций, предлагая время и место, а также повестку дня для последующего согласования со всеми Сторонами и Секретариатом Шанхайской организации сотрудничества.

3. Практическое взаимодействие по конкретным направлениям сотрудничества, предусмотренным настоящим Соглашением, Стороны могут осуществлять по линии компетентных органов государств Сторон, ответственных за реализацию Соглашения.

4. В целях создания правовых и организационных основ сотрудничества по конкретным направлениям компетентные органы государств Сторон могут заключать соответствующие договоры межведомственного характера.

Статья 6

Защита информации

1. Настоящее Соглашение не налагает на Стороны обязательств по предоставлению информации в рамках сотрудничества в соответствии с настоящим Соглашением и не является основанием для передачи информации в рамках этого сотрудничества, если раскрытие такой информации может нанести ущерб национальным интересам.

2. В рамках сотрудничества в соответствии с настоящим Соглашением Стороны не осуществляют обмен информацией, которая согласно законодательству государства любой из Сторон относится к государственной тайне и (или) государственным секретам. Порядок передачи и обращения с подобной информацией, которая в конкретных случаях может считаться необходимой для целей исполнения настоящего Соглашения, регулируется на основании и на условиях соответствующих договоров между Сторонами.

3. Стороны обеспечивают надлежащую защиту передаваемой или создаваемой в ходе сотрудничества в рамках настоящего Соглашения информации, не относящейся в соответствии с законодательством государства любой из Сторон к государственной тайне и (или) государственным секретам, доступ к которой и распространение которой ограничены в соответствии с законодательством и (или) соответствующими нормативно-правовыми актами государства любой из Сторон.

Защита такой информации осуществляется в соответствии с законодательством и (или) соответствующими нормативно-правовыми актами государства получающей Стороны. Такая информация не раскрывается и не передается без письменного согласия Стороны, являющейся источником этой информации.

Такая информация должным образом обозначается в соответствии с законодательством и (или) соответствующими нормативно-правовыми актами государств Сторон.

Статья 7

Финансирование

1. Стороны самостоятельно несут расходы по участию их представителей и экспертов в соответствующих мероприятиях по исполнению настоящего Соглашения.
2. В отношении прочих расходов, связанных с исполнением настоящего Соглашения, Стороны в каждом отдельном случае могут согласовывать иной порядок финансирования в соответствии с законодательством государств Сторон.

Статья 8

Отношение к другим международным договорам

Настоящее Соглашение не затрагивает прав и обязательств каждой из Сторон по другим международным договорам, участником которых является ее государство.

Статья 9

Разрешение споров

Стороны решают спорные вопросы, которые могут возникнуть в связи с толкованием или применением положений настоящего Соглашения, путем консультаций и переговоров.

Статья 10

Рабочие языки

Рабочими языками при осуществлении сотрудничества в рамках настоящего Соглашения являются русский и китайский языки.

Статья 11

Депозитарий

Депозитарием настоящего Соглашения является Секретариат Шанхайской организации сотрудничества.
Подлинный экземпляр настоящего Соглашения хранится у депозитария, который в течение пятнадцати дней с даты его подписания направит Сторонам его заверенные копии.

Статья 12

Заключительные положения

1. Настоящее Соглашение заключается на неопределенный срок и

вступает в силу на тридцатый день с даты получения депозитарием четвертого уведомления в письменной форме о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу. Для Стороны, выполнившей внутригосударственные процедуры позднее,

настоящее Соглашение вступает в силу на тридцатый день с даты получения депозитарием соответствующего уведомления.

2. Стороны могут вносить изменения в настоящее Соглашение, которые по взаимному согласию Сторон оформляются отдельным протоколом.

3. Настоящее Соглашение не направлено против каких-либо государств и организаций и после его вступления в силу открыто для присоединения любого государства, разделяющего цели и принципы настоящего Соглашения, путем передачи депозитарию документа о присоединении. Для присоединяющегося государства настоящее Соглашение вступает в силу по истечении тридцати дней с даты получения депозитарием последнего уведомления о согласии на такое присоединение подписавших его и присоединившихся к нему государств.

4. Каждая из Сторон может выйти из настоящего Соглашения, направив депозитарию в письменной форме уведомление об этом не менее чем за девяносто дней до предполагаемой даты выхода. Депозитарий извещает о таком намерении другие Стороны в течение тридцати дней с даты получения такого уведомления.

5. В случае прекращения действия настоящего Соглашения Стороны принимают меры для полного выполнения обязательств по защите информации, а также ранее согласованных совместных работ, проектов и иных мероприятий, осуществляемых в рамках Соглашения и не завершенных к моменту прекращения действия Соглашения.

Совершено в городе Екатеринбург 16 июня 2009 года в одном подлинном экземпляре на русском и китайском языках, причем оба текста имеют одинаковую силу.

(подписи)

ПРИЛОЖЕНИЕ 1
к Соглашению между правительствами государств—членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности

ПЕРЕЧЕНЬ

основных понятий в области обеспечения международной информационной безопасности

«Информационная безопасность» — состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;
«информационная война» — противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны;
«информационная инфраструктура» — совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации;
«информационное оружие» — информационные технологии, средства и методы, применяемые в целях ведения информационной войны;
«информационная преступность» — использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях;
«информационное пространство» — сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;
«информационные ресурсы» — информационная инфраструктура, а также собственно информация и ее потоки;
«информационный терроризм» — использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях;
«критически важные структуры» — объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо затрагивающие национальную безопасность, включая безопасность личности, общества и государства;

«международная информационная безопасность» — состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространств

«неправомерное использование информационных ресурсов» — использование информационных ресурсов без соответствующих прав или с нарушением установленных правил, законодательства государств Сторон либо норм международного права;
«несанкционированное вмешательство в информационные ресурсы» — неправомерное воздействие на процессы формирования, создания, обработки, преобразования, передачи, использования, хранения информации;
«угроза информационной безопасности» — факторы, создающие опасность для личности, общества, государства и их интересов в

ПРИЛОЖЕНИЕ 2
к Соглашению между правительствами государств—членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности

ПЕРЕЧЕНЬ
основных видов угроз в области международной информационной безопасности, их источников и признаков

1. Разработка и применение информационного оружия, подготовка и ведение информационной войны.
Источником этой угрозы являются создание и развитие информационного оружия, представляющего непосредственную угрозу для критически важных структур государств, что может привести к новой гонке вооружений и представляет главную угрозу в области международной информационной безопасности.
Ее признаками являются применение информационного оружия в целях подготовки и ведения информационной войны, а также воздействия на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться перед лицом агрессора и не может воспользоваться законным правом самозащиты; нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах; деструктивное воздействие на критически важные структуры.
2. Информационный терроризм.
Источником этой угрозы являются террористические организации и лица, причастные к террористической деятельности, осуществляющие противоправные действия посредством или в отношении информационных ресурсов.
Ее признаками являются использование информационных сетей террористическими организациями для осуществления террористической

деятельности и привлечения в свои ряды новых сторонников; деструктивное воздействие на информационные ресурсы, приводящее к нарушению общественного порядка; контролирование или блокирование каналов передачи массовой информации; использование сети Интернет или других информационных сетей для пропаганды терроризма, создания атмосферы страха и паники в обществе, а также иные негативные воздействия на информационные ресурсы.

3. Информационная преступность.

Источником этой угрозы являются лица или организации, осуществляющие неправомерное использование информационных ресурсов или несанкционированное вмешательство в такие ресурсы в преступных целях.

ANNEX 4: Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security

ty and possible cooperative measures to address them, as well as the concepts referred to in paragraph 2 above, and to submit a report on the results of this study to the General Assembly at its sixty-fifth session;

5. Decides to include in the provisional agenda of its sixty-fourth session the item entitled "Developments in the field of information and telecommunications in the context of international security".

61st plenary meeting
2 December 2008

AGREEMENT
between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security

Unofficial translation

The Governments of the Member States of the Shanghai Cooperation Organization hereinafter referred to as the Parties,

Noting considerable progress in the development and introduction of new information and communication technologies and means shaping the global information space,

Expressing concern about the threats posed by possible use of such technologies and means for the purposes incompatible with ensuring international security and stability in both civil and military spheres,

Attaching great importance to international information security as one of key elements of the system of international security,

Convinced that further enhancement of confidence and strengthening of interaction between the Parties in the field of ensuring international information security are urgently needed and serve the interests of the Parties,

Considering the important role of information security in the field of ensuring human and civil rights and fundamental freedoms,

Considering the resolutions of the UN General Assembly "Developments in the field of information and telecommunications in the context of international security",

Striving to curb international information security threats, ensure the information security interests of the Parties and create an international information environment of peace, cooperation and harmony,

Wishing to establish a legal and organizational framework for cooperation between the Parties in the field of ensuring international information security,

Have agreed as follows:

Article 1

General Terms

For the purpose of interaction between the Parties in the implementation of this Agreement, the basic terms shall be used which are listed in Annex 1 (List of Basic Terms in the Field of International Information Security) that is an integral part of this Agreement.

Annex 1 may, as necessary, be supplemented, amended and updated as agreed by the Parties.

Article 2

Main Threats in the Field of Ensuring International Information Security

In the process of cooperation in accordance with this Agreement the Parties shall proceed from the assumption that there are the following main threats in the field of ensuring international information security:

1) Development and use of information weapons, preparation for and waging information war;

2) Information terrorism;

3) Information crime;

4) Use of the dominant position in the information space to the detriment of the interests and security of other States;

5) Dissemination of information harmful to social and political, social and economic systems, as well as spiritual, moral and cultural spheres of other States;

6) Natural and/or man-made threats to safe and stable operation of global and national information infrastructures.

The agreed understanding by the Parties of the essence of major threats listed in this Article is provided in Annex 2 (List of Major International Information Security Threats, their Sources and Attributes) that is an integral part of this Agreement.

Annex 2 may, as necessary, be supplemented, amended and

updated as agreed by the Parties.

Article 3

Main Areas of Cooperation

Taking into account the threats under Article 2 of this Agreement, the Parties, their authorized representatives and competent authorities of the States of the Parties that are specified under Article 5 of this Agreement shall cooperate in ensuring international information security in the following main areas:

1) identifying, agreeing and implementing necessary collective measures in the field of ensuring international information security;

2) establishing a system to monitor and jointly respond to threats emerging in this area;

3) elaborating collective measures regarding development of norms of international law to curb proliferation and use of information weapons that endangers the defensive capability, national and public security;

4) countering threats of using ICTs for terrorist purposes;

5) countering information crime;

6) conducting examination, research and assessment in the field of ensuring information security that is necessary for the purposes of this Agreement;

7) assisting secure and stable functioning and internationalization of global Internet governance;

8) ensuring information security of critical structures of the States of the Parties;

9) elaborating and implementing joint confidence-building measures to ensure international information security;

10) elaborating and implementing coordinated policies and organizational and technical procedures for using the electronic digital signature and information protection in trans-border information exchange;

11) information exchange on legislation of the States of the Parties on issues of ensuring information security;

12) improving the international legal base and practical mechanisms of cooperation among the Parties in ensuring international information security;

13) creating conditions for interaction among the competent authorities of the States of the Parties in order to implement this Agreement;

14) interacting within the framework of international organizations and forums on ensuring international information security;

15) exchanging experience, training of specialists, holding working meetings, conferences, seminars and other forums of authorized representatives and experts of the Parties in the field of information security;

16) information exchange on issues concerning implementation of cooperation in the main areas listed in this Article.

The Parties or the competent authorities of the States of the Parties may determine other areas of cooperation by mutual agreement.

Article 4

General Principles of Cooperation

1. The Parties shall cooperate and act in the international information space within the framework of this Agreement in such a way that these activities contribute to social and economic development and comply with maintaining international security and stability, generally recognized principles and norms of international law, including the principles of peaceful settlement of disputes and conflicts, non-use of force, non-interference in internal affairs, respect for human rights and fundamental freedoms and the principles of regional cooperation and non-interference in the information resources of the States of the Parties.

2. The activities of the Parties within the framework of this Agreement should be compatible with the right of each Party to search, obtain and disseminate information given that this right can be restricted by law in order to protect national and public security.

3. Each Party shall have equal rights to protect the information resources and critical structures of their States from illicit use and unauthorized interference, including information attacks.

Each Party shall not carry out such actions against another Party and shall assist other Parties in exercising the above-mentioned right.

Article 5

Main Forms and Mechanisms of Cooperation

1. Within 60 days after the date on which this Agreement has entered into force, the Parties shall exchange data, through a depositary, on the competent authorities of the States of the Parties responsible for implementing this Agreement and channels of direct information exchange on specific areas of cooperation.

2. In order to review the implementation of this Agreement, information exchange, analysis and joint assessment of emerging threats to information security, as well as to determine, agree and coordinate joint response measures, the Parties should hold regular consultations between the authorized representatives of the Parties and competent authorities of the

States of the Parties (hereinafter - consultations).

Regular consultations shall be usually held, as agreed by the Parties, once in six months at the Secretariat of the Shanghai Cooperation Organization or in the territory of the State of one of the Parties at its invitation.

Any of the Parties may initiate extraordinary consultations proposing the time, venue and agenda for subsequent approval by all the Parties and the Secretariat of the Shanghai Cooperation Organization.

3. The Parties may engage in practical interaction in specific areas of cooperation provided for by this Agreement through the competent authorities of the States of the Parties responsible for implementing this Agreement.

4. In order to lay the legal and organizational foundation for cooperation in specific areas, the competent authorities of the States of the Parties may conclude appropriate interagency treaties.

Article 6

Protection of Information

1. This Agreement shall not oblige the Parties to provide information within the framework of cooperation in accordance with this Agreement and shall not provide basis for transferring information within the framework of this cooperation if the disclosure of such information might damage national interests.

2. Within the framework of cooperation in accordance with this Agreement, the Parties shall not exchange information that constitutes State secret and/or State secrets by law of the State of any of the Parties. The procedures of transferring and processing such information that may be considered necessary in certain cases for implementation of this Agreement shall be regulated subject to the terms and conditions of relevant treaties signed between the Parties.

3. The Parties shall ensure appropriate protection of the information transferred or generated in the course of cooperation within the framework of this Agreement, that shall not constitute State secret and/or State secrets according to the legislation of any of the States of the Parties, access and dissemination of which are restricted according to the legislation and/or relative regulations of any of the States of the Parties.

Such information shall be protected according to the legislation and/or relevant regulations of the State of the receiving Party. Such information shall not be disclosed or transferred without the written consent of the Party, which is the source of this information.

Such information shall be properly designated in accordance with the legislation and/or relevant regulations of the States of the Parties.

Article 7

Financing

1. The Parties shall independently bear the costs of participation of their representatives and experts in relevant activities relating to the implementation of this Agreement.

2. As for other costs of implementation of this Agreement, the Parties may agree upon other financing procedures in each particular case in accordance with the legislation of the States of the Parties.

Article 8

Relationship to other International Treaties

This Agreement shall not affect the rights and obligations of each of the Parties under other international Treaties to which their States are parties to.

Article 9

Settlement of Disputes

Disputes that may arise out of interpretation or application of the provisions of this Agreement shall be settled through consultations and negotiations.

Article 10

Working Languages

The working languages for cooperation under this Agreement shall be Russian and Chinese.

Article 11

Depositary

The Depositary of this Agreement shall be the Shanghai Cooperation Organization Secretariat.

The original copy of this Agreement shall be deposited with the Depositary that shall, within fifteen days following the date of its signature, send its certified copies to the Parties.

Article 12

Final Provisions

1. This Agreement shall be concluded for an indefinite period of time and enter into force on the thirtieth day following the date of receiving by the Depositary of the fourth written notification on the completion by the Parties of respective internal procedures necessary for its entry into force. For the Party that has completed its domestic procedures afterwards, this Agreement shall come into force on the thirtieth day from the date of receiving by the Depositary of the appropriate notification.

2. The Parties may amend this Agreement, which shall be formalized by mutual consent of the Parties, in a separate protocol.

3. This Agreement is not directed against any other States or organizations and upon its entering into force shall be open for accession by any State that shares the goals and principles of this Agreement, by depositing of the document of accession with the Depositary. For the acceding State, the present Agreement shall come into force on the thirtieth day following the date of receiving by the Depositary of the last notification of consent to such accession of both the signatory and acceding States.

4. Each Party can withdraw from this Agreement, by sending to the Depositary a written notification of its intention no less than ninety days before the expected date of withdrawal. The Depositary shall inform other Parties of this intention within thirty days from the date of receipt of such notification.

5. In case of termination of this Agreement the Parties shall undertake measures to fulfill their obligations on information security completely, as well as earlier agreed joint efforts, projects and other measures carried out under this Agreement and that have not been accomplished by the moment of the termination of this Agreement.

Done at Yekaterinburg on 16 June 2009 in a single original copy in Russian and Chinese, both texts being equally authentic.

For the Government
of the Republic of Kazakhstan

For the Government
of the People's Republic of China

For the Government
of the Kyrgyz Republic

For the Government
of the Russian Federation

For the Government
of the Republic of Tajikistan

For the Government
of the Republic of Uzbekistan

ANNEX 1
to the Agreement between the Governments
of the Member States of the Shanghai
Cooperation Organization on Cooperation
in the Field of International Information Security

LIST

of basic terms in the field of international information security

"Information security" - security of the individual, society, state and their interest from threats, destructive and other negative impacts in the information space;

"Information war" - confrontation between two or more states in the information space aimed at damaging information systems, processes and resources, critical and other structures, undermining political, economic and social systems, mass psychologic brainwashing to destabilize society and state, as well as to force the state to taking decisions in the interest of an opposing party;

"Information infrastructure" - array of technical means and systems to generate, transform, transfer, use and store information;

"Information weapon" - information technologies, ways and means of waging an information war;

"Information crime" - use of and/or attack on information resources in the information space for illegal purposes;

"Information space" - field of activities related to generating, transforming, transferring, using and storing information which influences, in particular, individual and public mind, information infrastructure and information as such;

"Information resources" - information infrastructure, as well as information as such and its flows;

"Information terrorism" - use of and/or attack on information resources in the information space for terrorist purposes;

"Critical structures" - public facilities, systems and institutions attacks on which may cause consequences directly affecting national security, including that of the individual, society and state;

"International information security" - international relations environment which rules out violating world stability

and threatening the security of states and world community in the information space;

"Unlawful use of information resources" - use of information resources without relevant rights or in violation of the existing rules and laws of states or norms of international law;

"Unauthorized interference with the information resources " - unlawful impact on the processes of generating, processing, transforming, transferring, using and storing information;

"Information security threat" - factors which pose a threat to the individual, society, state and their interest in the information space.

ANNEX 2
to the Agreement between the Governments
of the Member States of the Shanghai
Cooperation Organization on Cooperation
in the Field of International Information Security

LIST

of Major International Information Security Threats,
their Sources and Attributes

1. Development and use of information weapons, preparing and waging information war.

This threat emanates from creating and developing information weapons that pose an immediate danger to critical structures of States which might lead to a new arms race and represents a major threat in the field of international information security.

Among its characteristics are the use of information weapons to prepare and wage information war, and impact transportation, communication and air control systems, missile defense and other types of defense facilities, as a result of which the State looses its defense capabilities in the face of aggressor and fails to exercise its legitimate

right to self-defense; breaching information infrastructure operation, which leads to the collapse of administrative and decision-making systems in the States; and destructive impact on critical structures.

2. Information terrorism.

This threat emanates from terrorist organizations and individuals involved in terrorist activities acting unlawfully through information resources against regarding them.

It is characterized by the use of information networks by terrorist organizations to carry out terrorist activities and recruit new supporters; destructive impact on information resources leading to disruption of public order; control or blocking of mass media channels; use of the Internet or other information networks for terrorist propaganda, creating an atmosphere of fear and panic in the society, as well as other negative impacts on the information resources.

3. Information crime.

The sources of this threat include individuals or organizations involved in the unlawful use of information resources or unauthorized interference in such resources for criminal purposes.

It is characterized by breaching information systems to compromise information integrity, accessibility and confidentiality; deliberate production and dissemination of computer viruses and other malicious programs; DoS-attacks (denial of service) and other negative impacts; damage to information resources; violation of legitimate rights and freedoms of citizens in the information sphere, including intellectual property and privacy; use of information resources and methods in order to commit such crimes as fraud, theft, extortion, smuggling, illicit drug trafficking, distribution of child pornography, etc..

4. Use of dominant position in the information space to the detriment of the interests and security of other countries.

The sources of this threat include the uneven development of information technologies in various states and the existing trend to increase the "digital gap" between the developed and developing countries. A number of states that have advantages in the development of information technologies deliberately constrain the development of other countries and access to information technologies, which

creates a serious danger for the states with insufficient information potential.

It is characterized by monopolization of production of software and hardware of information infrastructures, limitation of state participation in international information technology cooperation which hampers their development and increases the dependence of these countries from the more developed states; embedding of hidden options and functions into the software and hardware supplied to other countries in order to control and influence information resources and/or critical structures of these countries; control and monopolization of the market of information technologies and products to the detriment of the interests and security of the States.

5. Dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States.

This threat emanates from states, organizations, groups of people or individuals that use the information infrastructure to disseminate information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States.

It is characterized by the appearance and replication of information in digital (radio and television) and other mass media, on the Internet and other information exchange networks that:

distorts the perception of the political system, social order, domestic and foreign policy, important political and social processes in the State, spiritual, moral and cultural values of its population;

promotes the ideas of terrorism, separatism and extremism;

stirs up inter-ethnic, interracial and inter-confessional hostility.

6. Natural and/or man-made threats to safe and stable operation of global and national information infrastructures.

These threats emanate from natural disasters and other dangerous natural phenomena, as well as man-made disasters that occur suddenly or as a result of a long process that can cause large-scale impact on the information resources of the State.

They are characterized by disruption of operation of information infrastructure facilities and, as a consequence, destabilization of critical structures, state management and decision-making systems, which directly affects state and social security.

Annex 5 – U.S. Agreements By Type

agreement_name	agreement_type	agreement_date	agreement_signatories	agreement_summary	source	Combo53
Technical Agreement Between NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team EU (CERT-EU)	Policy, Cyber Operations	02-Oct-16	Albania, Austria, Slovakia, Slovenia, Spain , Sweden, Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania	Improve cyber incident prevention, detection and response; EU has been observing the NATO annual cyber defense exercise, Cyber Coalition	-	CERT to CERT
NATO Cyber Defense Pledge	Information Sharing, Policy, Cyber Exercises, Training, Military	08-Jul-16	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Iceland, Italy, Latvia, Lithuania, Luxembourg, Norway, Portugal, Romania	Enhance cyber defenses and national infrastructures; Work with EU and other allies to enhance cyber defense cooperation; Partner with industry and academia; Emphasize cooperation via education, training, exercises, and information exchange	http://www.nato.int/cps/en/natohq/official_texts_133177.htm	Government to Government
Defense Agreement between the United States and Iceland	Military	29-Jun-16	United States of America, Iceland	Allows for DoD's plans for the defense of Iceland by military means, as well as addressing "issues of mutual interest such as cyber and maritime security, exchange of classified information, and others issues as mutually determined.	-	Government to Government

Framework for the United States-India Cyber Relationship	Cyber Crime, Information Sharing, Research, Best Practices, Cyber Exercises, Training	01-Jun-16	United States of America, India	Sharing best practices, sharing information on a real time or near real time basis, R&D, combat cyber crime, joint training programs, facilitating joint tabletop exercises.	-	Government to Government
Strategic Agreement between French electronics group Thales and US Cisco Systems	Information Sharing, Research	01-Jun-16	United States of America, France	Co-develop a solution to better detect and counter cyberattacks in real time; aimed first at French infrastructure providers, then to be deployed globally	-	Industry to Industry
Technical Cooperation Agreement between the Regional Association of Oil, Gas, and Biofuels Sector Companies in Latin America and the Caribbean (ARPEL) and the Industrial Cybersecurity Center of Spain	Information Sharing	29-Apr-16	Argentina, Spain , Suriname, Switzerland, United States of America, Uruguay, Venezuela, Bolivia, Chile, Colombia, Costa Rica, Ecuador, Ghana, Jamaica, Mexico, Netherlands, Paraguay	Address cybersecurity in critical infrastructure, share knowledge and experiences among professionals in the field to reduce vulnerabilities of companies to cyber attacks, build capacities for management of cybersecurity and the response to emergencies	-	Industry to Industry
Spain's National Institute for Cybersecurity (INCIBE) agreement with the University of Washington	Research	01-Apr-16	Spain , United States of America	Jointly run research projects on cybersecurity	-	Institution to Institution

APEC Telecommunications and Information Working Group Strategic Action Plan	Policy, Research, Cyber Operations	01-Jan-16	Australia, Singapore, Thailand, United States of America, Viet Nam, Brunei Darussalam, Canada, Chile, China, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Republic of Korea, Russian Federation, Hong Kong, Taiwan	Develop and support ICT innovation, promote a secure, resilient, and trusted ICT environment, promote regional economic integration, enhance digital economy and internet economy, strengthen cooperation	-	Government to Government
MoU between the Organization of American States and Spain	Cyber Crime, Information Sharing, Policy	16-Nov-15	Antigua and Barbuda, Argentina, Spain , Trinidad and Tobago, United States of America, Uruguay, Venezuela, Bahamas, Barbados, Belize, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines	Cooperation on cybersecurity and the fight against terrorism; Exchange information, develop initiatives of mutual interest, training, workshops, legislative assistance activities, conferences, and meetings. Fight against cyber crime and cyber terrorism	-	Government to Government
MoU among Hague Security Delta (Netherlands), Virginia Economic Development Partnership, and Fairfax County Economic Development Authority	Research	01-Oct-15	United States of America, Netherlands	Focus on cybersecurity research and development, as well as business cooperation; Part of the extended program of the joint Dutch-Flemish mission in Atlanta	-	Agency to Agency

US-China Cyber Agreement	Cyber Crime, Information Sharing	25-Sep-15	United States of America, China	Investigate cyber crimes and mitigate malicious activity emanating from each country's territory; refrain from knowingly stealing intellectual property; promote international state cybersecurity behavior norms; establish high-level joint dialogue to combat cyber crime and related issues	-	Government to Government
Joint Statement: 2015 United States-India 4th Cyber Dialogue	Cyber Crime, Research	11-Aug-15	United States of America, India	Increased collaboration on cybersecurity capacity-building, cybersecurity R&D, and in combatting cyber crime.	-	Government to Government
Microsoft-Spanish National Intelligence Center (CNI) agreement	Research	01-Jul-15	Spain , United States of America	Greater transparency in Microsoft's Government Security Program; Research to improve security against cyber attacks and vulnerabilities	-	Agency to Industry
US Trade and Development Agency (USTDA) Public-Private Partnership with CERT-RO (May 2015-present)	Research, Cyber Operations, Training	01-May-15	United States of America, Romania	Romanian government launched a cybersecurity innovation center (CIC) in partnership with USTDA in May 2015 to identify, assess and manage cyber risks; CIC will train personnel, test new technologies, simulate cyber attacks, and facilitate cross-regional trade opportunities for collaboration	-	Agency to CERT

Assessing and developing Cybersecurity Capability Initiative, Norway, United Kingdom, Organization of American States, Global Cybersecurity Capacity Center (GCSSC)	Best Practices	01-Apr-15	Antigua and Barbuda, Argentina, Trinidad and Tobago, United Kingdom of Great Britain and Northern Ireland, United States of America, Uruguay, Venezuela, Bahamas, Barbados, Belize, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Norway, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines	Aims to assist countries in understanding their priorities for investment and development to respond to cyber incidents using a Capability Maturity Model for qualitative and quantitative benchmarking; Five dimensions of the Capability Maturity Model: 1. Security strategy, defense and resilience, 2. Culture and society, 3. Knowledge development, 4. Law and regulation, 5. Standards, controls, and technologies	-	Government to Government
MoU between the United States Federal Trade Commission and the Dutch Data Protection Authority in the Enforcement of Laws Protecting Personal Information in the Private Sector	Information Sharing, Research, Training	06-Mar-15	United States of America, Netherlands	Cooperating when enforcing applicable privacy laws such as the FTC Act and the Dutch Data Protection Act, including sharing relevant information about complaints; Facilitating research and education about how to protect personal information; Aiding mutual exchange of knowledge and expertise between the two entities via training programs and staff exchanges; Informing each other of privacy-related developments	https://www.ftc.gov/system/files/documents/cooperation_agreements/150309ftcdutchcb-1.pdf	Agency to Agency

Agreement between Bulgarian Ministry of Defense and NATO Communications and Information Organization (NCIO)	Military	01-Jan-15	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	NCIO to support Bulgaria's NATO 2020 strategy with focus on Cyber Defense, automated information services modernization, and cryptographic equipment acquisition services	-	Agency to Agency
Estonia and Raytheon Cyber Agreement	Cyber Operations, Military	01-Jan-15	United States of America, Estonia	Advance defense industry partnerships and pursue collaborative initiatives to enhance Cyber Defense capabilities of Estonia	-	Government to Industry
Florida Atlantic University and South Korea Telecom research and education agreement	Research	01-Jan-15	United States of America, Republic of Korea	Collaborate on the development of secure communications using quantum physics for applications in cryptology, hardware engineering, and quantum computing	-	Agency to Industry
MoU on Cyber Defense Cooperation between NATO and the Czech Republic	Cyber Operations, Military	01-Jan-15	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Improve and enhance Cyber Defense cooperation; cooperate in fighting against cyber threats and attacks	-	Government to Government

Joint Cyber Crime Action Taskforce (J-CAT)	Cyber Crime	01-Sep-14	Austria, Spain , United Kingdom of Great Britain and Northern Ireland, United States of America, Canada, Finland, Germany, Italy, Netherlands	India to be Britain's "trusted partner" over cyber crime and security; Create a joint task force to exchange and share information about identifying and countering threats; Police training exchanges in cyber forensics and other areas of detection and enforcement; Regular cooperation meetings between leaders in cybersecurity research from academia and industry	-	Government to Government
Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security	Policy	02-Jul-14	Australia, Singapore, Spain , Sweden, Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, Pakistan, Republic of Korea	IT products and protection profiles that earn a Common Criteria Certificate, based on a collaborative Protection Profile (cPP) and Evaluation Assurance Levels, can be procured and used without further evaluation.	-	Government to Government
Boeing (USA) deal with Head Italia (Italian military intelligence and telecommunications supplier)	Information Sharing, Cyber Operations	01-Jun-14	United States of America, Italy	Provide Italian government and defense customers with advanced cybersecurity solutions to protect critical data and infrastructure; Provide training and simulation platforms; improve information security defense in face of cyber attacks or natural disasters.	-	Industry to Industry

Agreement between Microsoft and Mexico Federal Police to Take Action Against Cyber Crime	Cyber Crime	01-Jan-14	United States of America, Mexico	Cooperation against cyber crime	-	Agency to Industry
Individual Partnership and Cooperation Program between Japan and NATO	Research	01-Jan-14	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Cooperate and share lessons learned on Cyber Defense	http://www.nato.int/nato_static/assets/pdf/pdf_2014_05/20140507_140507-IPCP_Japan.pdf	Government to Government
NATO Cooperative Cyber Defense Centre of Excellence Signed Agreement with Estonian Defense League	Cyber Exercises, Military	01-Jan-14	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Formalizes existing partnership and the annual Cyber Defense exercises (Locked Shields)	Agency-Agency? Government-Agency?	Agency to Agency

Organization of American States (OAS) and Estonia MoU on Cybersecurity	Cyber Operations, Training	01-Jan-14	Antigua and Barbuda, Argentina, Trinidad and Tobago, United States of America, Uruguay, Venezuela, Bahamas, Barbados, Belize, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Estonia, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines	Promote development of cybersecurity capabilities in the Americas to include advising on the creation of cybersecurity documents and training	-	Government to Government
Security Cooperation Program (SCP) between Microsoft and ITPSS	Information Sharing, Cyber Operations, Training	01-Jan-14	United States of America, Brunei Darussalam	Brunei and Microsoft will engage in cooperative activities related to cybersecurity; online training and webinars on cybersecurity topics and information exchanges; computer incident response	-	CERT to Industry
US-Russian Cooperation on Information and Communications Technology and Security	Information Sharing, Cyber Operations	17-Jun-13	United States of America, Russian Federation	Conclude a range of steps designed to increase transparency and reduce escalation, have US-CERT and RUS-CERT exchange technical information; use the Nuclear Risk Reduction Center to build confidence through information exchange; authorize direct communications between the US Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council	Also CERT-CERT	Government to Government

R&D agreement between the Scientific and Technological Research Council of Turkey (TUBITAK) Informatics and Information Security Research Center (BILGEM) and NATO	Research	01-Jan-13	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania		-	Government to Industry
Individual Partnership and Cooperation Program between New Zealand and NATO	Information Sharing, Policy, Cyber Operations	27-Jun-12	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Romania	Develop common approaches to meet emerging security challenges (cyber given as an example)	http://www.nato.int/cps/ic/natohq/official_texts_88720.htm	Government to Government

US Department of Homeland Security-Dutch Ministry of Security and Justice Letter of Intent on Cybersecurity Cooperation	Cyber Operations	22-Feb-12	United States of America, Netherlands	Build upon cooperative cybersecurity initiatives to promote a safe, secure, and resilient cyber environment; Collaborate on incident management and response activities, control systems security, and cybersecurity exercises; DHS-Dutch National Cybersecurity Center meeting on February 21, 2012, identified cyber forensics, malicious software in a mobile environment, cross-border identity management, vital infrastructures/SCADA, and cloud computing as focus areas.	-	Agency to Agency
MoU between the Government of Latvia and NATO Concerning Cooperation on Cyber Defense	Cyber Operations	20-Jan-12	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Enhance the contribution of Latvia to international cooperation in the area of cybersecurity and defense in view of the cross-border nature of threats to information technologies	-	Government to Government

MoU between NATO Cyber Defense Management Board (CDMB) and National Security Authority of the Czech Republic Concerning Cooperation on Cyber Defense	Military	01-Jan-12	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania		No details found per word doc	Agency to Agency
Statement of Intent Regarding Cooperation on Cybersecurity and Cyber Incident Response	Information Sharing, Cyber Operations, Best Practices, Cyber Exercises, Training	01-Jan-12	Australia, United States of America	Enhance information sharing on operational cybersecurity issues among national cyber incident response teams; enhance crisis coordination; exchange best practices; share information on cyber exercises	-	Government to Government
Finmeccanica (Italy aerospace and defense) and Northrop Grumman (USA) Teaming Agreement	Cyber Operations	19-Dec-11	United States of America, Italy	Helps meet the requirements of the NATO Computer Incident Response Capability (NCIRC)-Full Operating Capability (FOC)	-	Industry to Industry

Poland Agreement with NATO Consultation, Command, and Control Agency	Research	24-Feb-11	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Facilitate joint research and development and lower the cost of Cyber Defense	-	Government to Agency
MoU between the United States and India	Information Sharing, Best Practices	19-Jan-11	United States of America, India	Promote closer cooperation and timely exchange of information; promote best practices for the exchange of critical cybersecurity information and expertise between the two governments through the Indian Computer Emergency Response Team (CERT-In), Department of Information Technology, Ministry of Communications and Information Technology, and DHS' United States Computer Emergency Readiness Team (US-CERT).	-	Government to Government

NATO and Estonia Agreement on Cyber Defense	Information Sharing, Policy, Military	01-Jan-10	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Agreement renewed in 2016; creates legal framework for Cyber Defense cooperation, facilitates information exchange, and provides mechanism for assistance in case of cyber attack	-	Government to Government
European Electronic Crime Task Force (EECTF) between the United States Secret Service and Italy's Postal and Communications Police, and the Public Security Department of the Italian Ministry of Interior	Cyber Crime	01-Jan-09	United States of America, Italy	Build a Europe-wide strategic alliance to fight and prosecute computer crime; Prevent identity theft, computer hacking and other computer-based crime; The task force will use the software that Poste Italiane developed that can track electronic payments as it moves beyond traditional mail delivery	-	Agency to Agency
Chile and Microsoft Security Cooperation Program	Information Sharing, Cyber Operations, Training	01-Jan-07	United States of America, Chile	Bring Microsoft expertise/training to Chilean government and educational institutions; goal of decreasing risk of security attacks; created ethical hacking challenges; CLCERT receives a notification when Microsoft has a malware alert	-	Government to Industry

MoU between the National Research Institute of Electronics and Cryptology (TUBITAK UEKAE) and NATO Computer Incident Response Capability- NCIRC	Cyber Operations, Cyber Exercises	15-Dec-06	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Access to the NCIRC network, participation to NATO Cyber Defense exercise, joint incident response, support on malicious code analysis, vulnerability database, alarm and warnings, staff exchanges	Agency-Institution?	Agency to Industry
US-India Cybersecurity Forum (2006)	Information Sharing	01-Jan-06	United States of America, India	Added cooperation in transportation and financial sectors; set up an India Information Sharing and Analysis Center and the India Anti-Bot Alliance	-	Government to Government
Lima Declaration	Policy, Cyber Operations, Best Practices	01-Jan-05	Australia, Singapore, Thailand, United States of America, Viet Nam, Brunei Darussalam, Canada, Chile, China, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Republic of Korea, Russian Federation, Hong Kong, Taiwan	Key principles for broadband development, compliance and enforcement principles, guiding principles for PKI-based approaches to electronic authentication, principles for action against spam and the implementation guidelines for action against spam	-	Government to Government

Budapest Convention on Cyber Crime	Cyber Crime	01-Jul-04	Albania, Andorra, Armenia, Australia, Austria, Slovakia, Slovenia, South Africa, Spain , Sri Lanka, Sweden, Switzerland, Turkey, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Monaco, Montenegro, Netherlands, Norway, Panama, Poland, Portugal, Romania, Serbia	First international treaty on crimes committed via the internet and other computer networks; dealing with infringements of copyright, computer-related fraud, child pornography, and violations of network security. Main objective is to pursue a common criminal policy against cyber crime	-	Government to Government
London Action Plan on International Spam Enforcement	Cyber Crime	01-Jan-04	Australia, South Africa, Spain , Sweden, Switzerland, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Brazil, Canada, Chile, China, Denmark, Finland, Hungary, Ireland, Japan, Latvia, Lithuania, Malaysia, Mexico, Netherlands, New Zealand, Nigeria, Norway, Portugal, Republic of Korea	Encourage communication and coordination among the agencies with spam enforcement authority; share findings with the OECD Spam Task Force	-	Government to Government

MoU on Mutual Enforcement Assistance in Commercial Email Matters	Cyber Crime	01-Jan-04	Australia, United Kingdom of Great Britain and Northern Ireland, United States of America	Facilitate effective enforcement against spam violations; facilitate investigations of spam violations; assist one another in providing evidence that could assist in determining whether a person has committed a spam violation; law enforcement assistance	-	Government to Government
US-India Cybersecurity Forum (2004)	Cyber Crime, Research, Cyber Operations, Military	01-Jan-04	United States of America, India	Established five joint working groups to cover legal cooperation and law enforcement, research and development, critical information infrastructure, watch and warning emergency response, defense cooperation, and standards and software assurance.	-	Government to Government
APEC Cybersecurity Strategy	Information Sharing, Best Practices, Training	01-Jan-02	Australia, Singapore, Thailand, United States of America, Viet Nam, Brunei Darussalam, Canada, Chile, China, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Republic of Korea, Russian Federation, Hong Kong, Taiwan	Recommendtions in information sharing and cooperation, security and technical guidelines, public awareness, training, and education	-	Government to Government

US-India Cybersecurity Forum (2001)	Information Sharing, Cyber Operations	01-Jan-01	United States of America, India	CERT-In and US National Cybersecurity Division share expertise in artifact analysis, network traffic analysis, and exchange of information; US-India High Technology Cooperation Group formed in 2002	-	Government to Government
National Guard State Partnership between Hungary and Ohio	Information Sharing	01-Jan-93	United States of America, Hungary	One of the 22 European partnerships of U.S. European Command (EUCOM) State Partnership Program, given the large population of Hungarians throughout Ohio; EUCOM Cyber Defense-staff assistance visit (SAV): U.S. Air Force Tech. Sgt. Steven Schwarck, cyberspace operations, 121st Air Refueling Wing Communications Flight, travelled to Budapest, Hungary in September 2015 as part of the National Guard State Partnership Program. He met with the Hungarian Military National Security Service to discuss Cyber Defense topics. "We discussed our methods of cybersecurity - our architecture, solutions and software, and we also explained aspects of DoD 8570, which provides guidance on training for DoD staff," said Tech. Sgt. Schwarck.	-	Government to Government

Best Practices	6
Cyber Crime	11
Cyber Exercises	5
Cyber Operations	18
Information Sharing	19
Military	9
Policy	7
Research	14
Training	9
AGREEMENTS W/ DOUBLE-COUNTS	98

ANNEX 6 – China Agreements By Type

agreement_name	agreement_type	agreement_date	agreement_signatories	agreement_summary	source	Combo53
China-Germany Pending Cybersecurity Agreement	Policy	01-Jun-16	China, Germany	Agreement to aid "Made in China 2025" and German "Industry 4.0" initiatives; Refraining from economic cyber espionage; Developing a mechanism for dealing with possible breaches, e.g. espionage, with a control mechanism set up to monitor possible incidents; Possibly reached in June 2016 (unconfirmed news reports)	-	Government to Government
MoU Between Malta Government and Huawei (China)	Research, Training	16-Apr-16	China, Malta	Strategic alliance agreement to support the Digital Malta program; 3 main areas of cooperation: creation of a joint innovation center in Malta for R&D of smart city solutions to prevent and react to evolving threats; Plan to deploy a 4.5G commercial pilot with telecom operators in Malta, and offering two weeks of ICT training in China for 5 talented Maltese students.	-	Government to Industry
MoU between Spanish National Institute of Cybersecurity (INCIBE) and Huawei Spain (China)	Best Practices, Training	26-Feb-16	Spain , China	First Huawei agreement with a European country; Periodically share information regarding cybersecurity actions and protection measures, and best practices, promote awareness and training in cybersecurity; Support the training and qualification of Spanish companies and professionals		Industry to Industry

APEC Telecommunications and Information Working Group Strategic Action Plan	Policy, Research, Cyber Operations	01-Jan-16	Australia, Singapore, Thailand, United States of America, Viet Nam, Brunei Darussalam, Canada, Chile, China, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Republic of Korea, Russian Federation, Hong Kong, Taiwan	Develop and support ICT innovation, promote a secure, resilient, and trusted ICT environment, promote regional economic integration, enhance digital economy and internet economy, strengthen cooperation	-	Government to Government
Cooperation on Cybersecurity between China and Indonesia	Information Sharing, Research, Cyber Operations	01-Jan-16	China, Indonesia	Information and communication technology strategy (cybersecurity awareness for decision-making purposes and cybersecurity in national infrastructure development); capacity building in operations and technology (in digital forensics, information security, network security, cyber risk management, big data analysis, and the digital economy); joint research in cybersecurity (cryptography operating systems, cyber law, cyber terrorism, and counter cyber intelligence); joint operations (cyber war simulation, response and mitigation in cyber war, cyber monitoring, cyber crisis management, and resilience)	-	Government to Government
Joint Statement between the Indian Ministry of Home Affairs and the Ministry of Public Security for the People's Republic of China	Cyber Crime	21-Nov-15	China, India	Strengthen cooperation on cyber crime including telecom fraud, exchange visits, and cooperation in law enforcement capacity building.	-	Government to Government

UK-China Joint Statement on building a global comprehensive strategic partnership for the 21st century	Cyber Crime	22-Oct-15	United Kingdom of Great Britain and Northern Ireland, China	Establish high-level dialogues to strengthen cooperation on cyber crime; agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information	https://www.gov.uk/government/news/uk-china-joint-statement-2015	Government to Government
US-China Cyber Agreement	Cyber Crime, Information Sharing	25-Sep-15	United States of America, China	Investigate cyber crimes and mitigate malicious activity emanating from each country's territory; refrain from knowingly stealing intellectual property; promote international state cybersecurity behavior norms; establish high-level joint dialogue to combat cyber crime and related issues	-	Government to Government
Joint Statement on Strengthening Comprehensive Strategic Partnership between the People's Republic of China and the Republic of Indonesia	Cyber Crime	27-Mar-15	China, Indonesia	Enhance cooperation in cybersecurity; cooperate on countering cyberterrorism	http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/t1249201.shtml	Government to Government
China-Russia Bilateral Agreement	Cyber Crime, Information Sharing, Policy, Research, Training	01-Jan-15	China, Russian Federation	Oppose the use of information technology in internal affairs of other states and to undermine national sovereignty	http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf	Government to Government

Cooperation agreement between Russia's Kaspersky Lab and China's Zhongguo Wangan	Cyber Operations	01-Jan-15	China, Russian Federation	Cooperation on quality software protecting China from cyber attack	-	Industry to Industry
Joint Statement on Strengthening Comprehensive Strategic Partnership between the PRC and The Republic of Indonesia	Cyber Crime, Information Sharing	01-Jan-15	China, Indonesia	Enhance cooperation in cybersecurity; cooperate on countering cyberterrorism	-	Government to Government
MoU between China and Laos on Cyberspace Cooperation and Development		01-Jan-15	China, Lao People's Democratic Republic		-	Government to Government
China and Tajikistan Joint Declaration	Information Sharing	01-Jan-14	Tajikistan, China	Maintain close communication and increase cooperation in cybersecurity	-	Government to Government
MoU between South Korea's Ministry of Science, ICT & Future Planning, and China's Ministry of Industry and Information Technology	Information Sharing, Research, Training	01-Jan-14	China, Republic of Korea	Form a cooperative group to jointly respond to APT, phishing, and DDoS attacks; conduct joint research; share information on cyber threats; exchange cybersecurity specialists	-	Agency to Agency

EU-China 2020 Strategic Agenda for Cooperation	Cyber Crime	01-Jan-13	Austria, Slovakia, Slovenia, Spain , Sweden, United Kingdom of Great Britain and Northern Ireland, Belgium, Bulgaria, China, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania	Support and promote peaceful, secure, and resilient open cyber space through EU-China Cyber Taskforce; collaborate on projects combatting cyber-crime	http://eeas.europa.eu/archives/docs/china/docs/20131123_agenda_2020_en.pdf	Government to Government
MoU between CERT Australia and CERT China	Cyber Operations	01-Jan-13	Australia, China	Enhance information sharing; streamline priority incident handling	-	CERT to CERT
Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security	Cyber Crime, Information Sharing, Policy	01-Jan-09	Tajikistan, Uzbekistan, China, Kazakhstan, Kyrgyzstan, Russian Federation	Found unofficial English translation Establish a system to monitor and respond to emerging cyber threats Curb the use of information weapons which endanger security and defense Counter information crime Ensure information security of critical structures belonging to signatories Elaborate upon and coordinate policies and procedures using electronic digital signature and information protection in trans-border information exchange Exchange of experience and training of specialists	-	Government to Government

MoU between ASEAN and China on Cooperation in the Field of non-traditional security issues	Cyber Crime, Information Sharing, Research, Training	01-Jan-09	Singapore, Thailand, Viet Nam, Brunei Darussalam, Cambodia, China, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, Philippines	Information sharing, personnel exchange and training, law enforcement, joint research	http://www.asean.org/storage/images/archive/documents/ASEAN-ChinaMOUonNTS.pdf	Government to Government
Lima Declaration	Policy, Cyber Operations, Best Practices	01-Jan-05	Australia, Singapore, Thailand, United States of America, Viet Nam, Brunei Darussalam, Canada, Chile, China, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Republic of Korea, Russian Federation, Hong Kong, Taiwan	Key principles for broadband development, compliance and enforcement principles, guiding principles for PKI-based approaches to electronic authentication, principles for action against spam and the implementation guidelines for action against spam	-	Government to Government
Seoul-Melbourne Multilateral MoU on Cooperation in Countering Spam	Information Sharing	01-Jan-05	Australia, Thailand, China, Japan, Malaysia, New Zealand, Philippines, Republic of Korea	Twelve Asia-Pacific communications and Internet agencies	-	Agency to Agency

London Action Plan on International Spam Enforcement	Cyber Crime	01-Jan-04	Australia, South Africa, Spain , Sweden, Switzerland, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Brazil, Canada, Chile, China, Denmark, Finland, Hungary, Ireland, Japan, Latvia, Lithuania, Malaysia, Mexico, Netherlands, New Zealand, Nigeria, Norway, Portugal, Republic of Korea	Encourage communication and coordination among the agencies with spam enforcement authority; share findings with the OECD Spam Task Force	-	Government to Government
APEC Cybersecurity Strategy	Information Sharing, Best Practices, Training	01-Jan-02	Australia, Singapore, Thailand, United States of America, Viet Nam, Brunei Darussalam, Canada, Chile, China, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Republic of Korea, Russian Federation, Hong Kong, Taiwan	Recommendtions in information sharing and cooperation, security and technical guidelines, public awareness, training, and education	-	Government to Government

23 TOTAL AGREEMENTS	
Best Practices	3
Cyber Crime	10
Cyber Exercises	0
Cyber Operations	5
Information Sharing	10
Military	0
Policy	4
Research	6
Training	6
AGREEMENTS W/ DOUBLE-COUNTS**	44

ANNEX 7 – Russia Agreements by Type

agreement_name	agreement_type	agreement_date	agreement_signatories	agreement_summary	source	Combo53
APEC Telecommunications and Information Working Group Strategic Action Plan	Policy, Research, Cyber Operations	01-Jan-16	Australia, Singapore, Thailand, United States of America, Viet Nam, Brunei Darussalam, Canada, Chile, China, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Republic of Korea, Russian Federation, Hong Kong, Taiwan	Develop and support ICT innovation, promote a secure, resilient, and trusted ICT environment, promote regional economic integration, enhance digital economy and internet economy, strengthen cooperation	-	Government to Government
China-Russia Bilateral Agreement	Cyber Crime, Information Sharing, Policy, Research, Training	01-Jan-15	China, Russian Federation	Oppose the use of information technology in internal affairs of other states and to undermine national sovereignty	http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf	Government to Government
Cooperation agreement between Russia's Kaspersky Lab and China's Zhongguo Wangan	Cyber Operations	01-Jan-15	China, Russian Federation	Cooperation on quality software protecting China from cyber attack	-	Industry to Industry
India-Russian Cooperation	Cyber Crime, Information Sharing, Training	01-Jan-15	India, Russian Federation	Set up an expert group on cybersecurity and counterterrorism; exchange of information and cooperation monitoring ISIL activity in cyber realm (Jihadi chat and online recruitment)	-	Government to Government

Iran-Russian Cooperation	Information Sharing, Military	01-Jan-15	Iran, Russian Federation	Agree to interact in Cyber Defense cooperation, specifically in areas of exchange and intelligence, interaction against threats, and joint defense	-	Government to Government
Druzhba-Dosti: A Vision for Strengthening the Indian-Russian Partnership over the Next Decade-Joint Statement	Policy, Cyber Operations	01-Jan-14	India, Russian Federation	Collaborate to promote safe, secure, and sustainable use of ICTs (information and communication technology) globally	http://pib.nic.in/newsite/PrintRelease.aspx?relid=113166	Government to Government
Japan-Russia Joint Press Conference	Training	01-Jan-14	Japan, Russian Federation	Launch a cybersecurity council; work in coordination in multilateral frameworks (ASEAN Regional Forum and Defense Ministers Meeting-Plus, East Asia Summit); regular expert level consultations on cybersecurity	-	Government to Government
US-Russian Cooperation on Information and Communications Technology and Security	Information Sharing, Cyber Operations	17-Jun-13	United States of America, Russian Federation	Conclude a range of steps designed to increase transparency and reduce escalation, have US-CERT and RUS-CERT exchange technical information; use the Nuclear Risk Reduction Center to build confidence through information exchange; authorize direct communications between the US Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council	Also CERT-CERT	Government to Government

Japan-Russia Joint Press Conference	Information Sharing	01-Jan-13	Japan, Russian Federation	First "2+2" meeting held and both sides agreed to launch a cybersecurity council; work in coordination in multilateral frameworks (ASEAN regional forum, East Asia Summit, ASEAN Defense Ministers Meeting-Plus); Regular expert level consultations on cybersecurity	http://www.mod.go.jp/e/pressconf/2013/11/131102.html	Government to Government
Agreement among the Governments of the SCO Member States on Cooperation in the Field of Ensuring International Information Security	Cyber Crime, Information Sharing, Policy	01-Jan-09	Tajikistan, Uzbekistan, China, Kazakhstan, Kyrgyzstan, Russian Federation	Found unofficial English translation Establish a system to monitor and respond to emerging cyber threats Curb the use of information weapons which endanger security and defense Counter information crime Ensure information security of critical structures belonging to signatories Elaborate upon and coordinate policies and procedures using electronic digital signature and information protection in trans-border information exchange Exchange of experience and training of specialists	-	Government to Government

Lima Declaration	Policy, Cyber Operations, Best Practices	01-Jan-05	Australia, Singapore, Thailand, United States of America, Viet Nam, Brunei Darussalam, Canada, Chile, China, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Republic of Korea, Russian Federation, Hong Kong, Taiwan	Key principles for broadband development, compliance and enforcement principles, guiding principles for PKI-based approaches to electronic authentication, principles for action against spam and the implementation guidelines for action against spam	-	Government to Government
APEC Cybersecurity Strategy	Information Sharing, Best Practices, Training	01-Jan-02	Australia, Singapore, Thailand, United States of America, Viet Nam, Brunei Darussalam, Canada, Chile, China, Indonesia, Japan, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Republic of Korea, Russian Federation, Hong Kong, Taiwan	Recommendtions in information sharing and cooperation, security and technical guidelines, public awareness, training, and education	-	Government to Government

12 TOTAL AGREEMENTS

Best Practices	2
Cyber Crime	3
Cyber Exercises	0
Cyber Operations	4
Information Sharing	7
Military	1
Policy	4
Research	1
Training	4
AGREEMENTS W/ DOUBLE-COUNTS	26

ANNEX 8 – U.K. Agreements By Type

agreement_name	agreement_type	agreement_date	agreement_signatories	agreement_summary	source	Combo53
Technical Agreement Between NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team EU (CERT-EU)	Policy, Cyber Operations	02-Oct-16	Albania, Austria, Slovakia, Slovenia, Spain , Sweden, Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania	Improve cyber incident prevention, detection and response; EU has been observing the NATO annual cyber defense exercise, Cyber Coalition	-	CERT to CERT
NATO Cyber Defense Pledge	Information Sharing, Policy, Cyber Exercises, Training, Military	08-Jul-16	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Iceland, Italy, Latvia, Lithuania, Luxembourg, Norway, Portugal, Romania	Enhance cyber defenses and national infrastructures; Work with EU and other allies to enhance cyber defense cooperation; Partner with industry and academia; Emphasize cooperation via education, training, exercises, and information exchange	http://www.nato.int/cps/en/natohq/official_texts_133177.htm	Government to Government

The EU Directive on security of network and information systems	Information Sharing, Policy, Cyber Operations	06-Jul-16	Austria, Slovakia, Slovenia, Spain , Sweden, United Kingdom of Great Britain and Northern Ireland, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania	Ensures member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority; Ensures cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to set a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks; Ensures a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.	-	Government to Government

European Commission Agreement with the European Cybersecurity Organization	Research, Cyber Operations	05-Jul-16	Austria, Slovakia, Slovenia, Spain , Sweden, United Kingdom of Great Britain and Northern Ireland, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania	Public-private partnership to better equip Europe against cyber attacks and strengthen competitiveness of its cybersecurity sector; 450 million Euro budget under the Horizon 2020 research and innovation program	-	Agency to Agency
EU-Malaysia Partnership and Cooperation Agreement (PCA)	Cyber Operations	06-Apr-16	Austria, Slovakia, Slovenia, Spain , Sweden, United Kingdom of Great Britain and Northern Ireland, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Netherlands, Poland, Portugal, Romania	Cooperation in cybersecurity issues	https://eeas.europa.eu/headquarters/headquarters-homepage/5348_en	Government to Government
Commonwealth Scientific and Industrial Research Organization (CSIRO) Data 61 and Cyber London MoU	Research	01-Apr-16	Australia, United Kingdom of Great Britain and Northern Ireland	Share expertise, resources, and capital to boost cybersecurity innovation to increase growth of industry; develop programs for improved cyber skills and governance; launch CyLon accelerator program in Australia to build a "regional powerhouse in cybersecurity"	-	Government to Government

MoU between Cyber London and Data61	Policy, Research	01-Apr-16	Australia, United Kingdom of Great Britain and Northern Ireland	Cylon, Europe's first cybersecurity accelerator (hub for training to entrepreneurs in cybersecurity companies), and Data61, largest data innovation group (data centric R&D) in Australia, agreed to launch a Cylon accelerator program in Australia, develop programs for improved cyber skills and governance, reciprocal landing pads to enable cyber innovation to be showcased to both buyers and investment capital in each nation.	-	Industry to Industry
Joint Statement between India and the UK	Cyber Crime, Training	01-Nov-15	United Kingdom of Great Britain and Northern Ireland, India	Work together to educate and train cybersecurity professionals; expand the UK's Cheyening Cyber Scholarships program for India; establish a cybersecurity training center of excellence; UK will provide advice on setting up the Indian Cyber Crime Coordination Center; Early conclusion of an MoU on CERT to CERT cooperation	-	Government to Government
UK-China Joint Statement on building a global comprehensive strategic partnership for the 21st century	Cyber Crime	22-Oct-15	United Kingdom of Great Britain and Northern Ireland, China	Establish high-level dialogues to strengthen cooperation on cyber crime; agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information	https://www.gov.uk/government/news/uk-china-joint-statement-2015	Government to Government

Assessing and developing Cybersecurity Capability Initiative, Norway, United Kingdom, Organization of American States, Global Cybersecurity Capacity Center (GCSSC)	Best Practices	01-Apr-15	Antigua and Barbuda, Argentina, Trinidad and Tobago, United Kingdom of Great Britain and Northern Ireland, United States of America, Uruguay, Venezuela, Bahamas, Barbados, Belize, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Norway, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines	Aims to assist countries in understanding their priorities for investment and development to respond to cyber incidents using a Capability Maturity Model for qualitative and quantitative benchmarking; Five dimensions of the Capability Maturity Model: 1. Security strategy, defense and resilience, 2. Culture and society, 3. Knowledge development, 4. Law and regulation, 5. Standards, controls, and technologies	-	Government to Government
Agreement between BAE Systems Applied Intelligence and Cybersecurity Malaysia	Policy, Training	01-Jan-15	United Kingdom of Great Britain and Northern Ireland, Malaysia	Established framework for cybersecurity collaboration; funds post-graduate program in cybersecurity at the National Defense University in Malaysia	-	Agency to Industry
Agreement between Bulgarian Ministry of Defense and NATO Communications and Information Organization (NCIO)	Military	01-Jan-15	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	NCIO to support Bulgaria's NATO 2020 strategy with focus on Cyber Defense, automated information services modernization, and cryptographic equipment acquisition services	-	Agency to Agency

MoU between Cybersecurity Agency (CSA - Singapore) and UK National Security Advisor	Research, Cyber Operations, Cyber Exercises	01-Jan-15	Singapore, United Kingdom of Great Britain and Northern Ireland	Incident response; talent development; joint cyber research and development collaboration - funded 6 research joint projects between Singapore Universities and UK Universities in areas of security and privacy in smart grid systems, vulnerability discovery, computational modeling and automatic non-intrusive detection of human behavior-based insecurity, creating synergistic capabilities in cybersecurity research, security by design for interconnected critical infrastructures, cybersecurity solutions for smart traffic control	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/485834/Singapore-UK_Joint_Grant_Call_Press_Release.pdf	Agency to Agency
MoU between Japan's National Institute of Communication and Technology (NICT) and UK Cybersecurity Academic Centers of Excellence	Research	01-Jan-15	United Kingdom of Great Britain and Northern Ireland, Japan	Cooperate on cyber research	-	Industry to Industry
MoU between the United Kingdom and Uzbekistan on Fighting Crime	Cyber Crime	01-Jan-15	United Kingdom of Great Britain and Northern Ireland, Uzbekistan	Includes cooperation in cyber crime	-	Government to Government

MoU on Cyber Defense Cooperation between NATO and the Czech Republic	Cyber Operations, Military	01-Jan-15	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Improve and enhance Cyber Defense cooperation; cooperate in fighting against cyber threats and attacks	-	Government to Government
UK-Qatar Security Pact	Informatio n Sharing	01-Nov-14	United Kingdom of Great Britain and Northern Ireland, Qatar	Share classified intelligence and deepen ties between security agencies to combat Jihadism and cyber warfare Enhance cooperation on digital defense	-	Government to Government
Joint Cyber Crime Action Taskforce (J-CAT)	Cyber Crime	01-Sep-14	Austria, Spain , United Kingdom of Great Britain and Northern Ireland, United States of America, Canada, Finland, Germany, Italy, Netherlands	India to be Britain's "trusted partner" over cyber crime and security; Create a joint task force to exchange and share information about identifying and countering threats; Police training exchanges in cyber forensics and other areas of detection and enforcement; Regular cooperation meetings between leaders in cybersecurity research from academia and industry	-	Government to Government
Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security	Policy	02-Jul-14	Australia, Singapore, Spain , Sweden, Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, Pakistan, Republic of Korea	IT products and protection profiles that earn a Common Criteria Certificate, based on a collaborative Protection Profile (cPP) and Evaluation Assurance Levels, can be procured and used without further evaluation.	-	Government to Government

UK-Japan Joint Statement: A Dynamic Strategic Partnership for the 21st century	Best Practices	01-May-14	United Kingdom of Great Britain and Northern Ireland, Japan	Work closely in areas of security, policing, and cybersecurity, given UK's experience of hosting the London 2012 Olympics to assist Tokyo 2020 Games; Continue UK-Japan Cyber Dialogue.	https://www.gov.uk/government/news/uk-japan-joint-statement	Government to Government
Canada-EU Strategic Partnership Agreement	Cyber Crime	01-Jan-14	Austria, Slovakia, Slovenia, Spain , Sweden, United Kingdom of Great Britain and Northern Ireland, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania	Cooperation against cyber crime	-	Government to Government
Individual Partnership and Cooperation Program between Japan and NATO	Research	01-Jan-14	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Cooperate and share lessons learned on Cyber Defense	http://www.nato.int/nato_static/assets/pdf/pdf_2014_05/20140507_140507-IPCP_Japan.pdf	Government to Government

Japan-EU Cyber Dialogue	Policy	01-Jan-14	Austria, Slovakia, Slovenia, Spain , Sweden, United Kingdom of Great Britain and Northern Ireland, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania		No information included in word doc	Government to Government
NATO Cooperative Cyber Defense Centre of Excellence Signed Agreement with Estonian Defense League	Cyber Exercises, Military	01-Jan-14	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Formalizes existing partnership and the annual Cyber Defense exercises (Locked Shields)	Agency-Agency? Government-Agency?	Agency to Agency
UK Cyber Crime deal with India	Cyber Crime, Information Sharing, Training	19-Feb-13	United Kingdom of Great Britain and Northern Ireland, India	India to be Britain's "trusted partner" over cyber crime and security; Create a joint task force to exchange and share information about identifying and countering threats; Police training exchanges in cyber forensics and other areas of detection and enforcement; Regular cooperation meetings between leaders in cybersecurity research from academia and industry	-	Government to Government

EU-China 2020 Strategic Agenda for Cooperation	Cyber Crime	01-Jan-13	Austria, Slovakia, Slovenia, Spain , Sweden, United Kingdom of Great Britain and Northern Ireland, Belgium, Bulgaria, China, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania	Support and promote peaceful, secure, and resilient open cyber space through EU-China Cyber Taskforce; collaborate on projects combatting cyber-crime	http://eeas.europa.eu/archives/docs/china/docs/20131123_agenda_2020_en.pdf	Government to Government
MoU between Republic of Korea and United Kingdom on IT cooperation	Policy	01-Jan-13	United Kingdom of Great Britain and Northern Ireland, Republic of Korea	Cooperate on cybersecurity issues	-	Government to Government
New Zealand-United Kingfom Joint Statement on Cybersecurity	Information Sharing, Policy, Cyber Operations	01-Jan-13	United Kingdom of Great Britain and Northern Ireland, New Zealand	Information sharing (to include intelligence); cyber-related research and development activities; coordinate responses to incidents	http://community.scoop.co.nz/2013/01/nz-uk-joint-statement-on-cyber-security/	Government to Government

R&D agreement between the Scientific and Technological Research Council of Turkey (TUBITAK) Informatics and Information Security Research Center (BILGEM) and NATO	Research	01-Jan-13	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania		-	Government to Industry
Individual Partnership and Cooperation Program between New Zealand and NATO	Information Sharing, Policy, Cyber Operations	27-Jun-12	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Romania	Develop common approaches to meet emerging security challenges (cyber given as an example)	http://www.nato.int/cps/ic/natohq/official_texts_88720.htm	Government to Government
MoU between the Government of Latvia and NATO Concerning Cooperation on Cyber Defense	Cyber Operations	20-Jan-12	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Enhance the contribution of Latvia to international cooperation in the area of cybersecurity and defense in view of the cross-border nature of threats to information technologies	-	Government to Government

MoU between NATO Cyber Defense Management Board (CDMB) and National Security Authority of the Czech Republic Concerning Cooperation on Cyber Defense	Military	01-Jan-12	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania		No details found per word doc	Agency to Agency
Cooperation agreement between the Scientific and Technological Research Council of Turkey (TUBITAK) and the Warwick Manufacturing Group (WMG) at the University of Warwick (UK)	Research	27-Oct-11	Turkey, United Kingdom of Great Britain and Northern Ireland	R&D and technology transfer in cybersecurity, education programs	Agency-Industry	
MoU Between Malaysia and the UK to Fight Cyber Crime	Cyber Crime, Information Sharing	01-Jul-11	United Kingdom of Great Britain and Northern Ireland, Malaysia	Work together to battle web-based crime, money laundering among other things; Set up technical cooperation and sharing of intelligence and expertise	-	Government to Government

Poland Agreement with NATO Consultation, Command, and Control Agency	Research	24-Feb-11	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Facilitate joint research and development and lower the cost of Cyber Defense	-	Government to Agency
EU and Korea Framework Agreement	Cyber Crime, Information Sharing, Research, Training	01-Jan-10	Austria, Slovakia, Slovenia, Spain , Sweden, United Kingdom of Great Britain and Northern Ireland, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Republic of Korea, Romania	Cooperate on cyber crime; exchange information on education and training of cyber crime investigators; investigation of cyber crime and digital forensics science	http://eeas.europa.eu/archives/docs/korea_south/docs/framework_agreement_final_en.pdf	Government to Government
NATO and Estonia Agreement on Cyber Defense	Information Sharing, Policy, Military	01-Jan-10	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Agreement renewed in 2016; creates legal framework for Cyber Defense cooperation, facilitates information exchange, and provides mechanism for assistance in case of cyber attack	-	Government to Government

MoU between the National Research Institute of Electronics and Cryptology (TUBITAK UEKAE) and NATO Computer Incident Response Capability- NCIRC	Cyber Operations, Cyber Exercises	15-Dec-06	Albania, Slovakia, Slovenia, Spain , Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania	Access to the NCIRC network, participation to NATO Cyber Defense exercise, joint incident response, support on malicious code analysis, vulnerability database, alarm and warnings, staff exchanges	Agency-Institution?	Agency to Industry
Budapest Convention on Cyber Crime	Cyber Crime	01-Jul-04	Albania, Andorra, Armenia, Australia, Austria, Slovakia, Slovenia, South Africa, Spain , Sri Lanka, Sweden, Switzerland, Turkey, Ukraine, United Kingdom of Great Britain and Northern Ireland, United States of America, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mauritius, Monaco, Montenegro, Netherlands, Norway, Panama, Poland, Portugal, Romania, Serbia	First international treaty on crimes committed via the internet and other computer networks; dealing with infringements of copyright, computer-related fraud, child pornography, and violations of network security. Main objective is to pursue a common criminal policy against cyber crime	-	Government to Government

London Action Plan on International Spam Enforcement	Cyber Crime	01-Jan-04	Australia, South Africa, Spain , Sweden, Switzerland, United Kingdom of Great Britain and Northern Ireland, United States of America, Belgium, Brazil, Canada, Chile, China, Denmark, Finland, Hungary, Ireland, Japan, Latvia, Lithuania, Malaysia, Mexico, Netherlands, New Zealand, Nigeria, Norway, Portugal, Republic of Korea	Encourage communication and coordination among the agencies with spam enforcement authority; share findings with the OECD Spam Task Force	-	Government to Government
MoU on Mutual Enforcement Assistance in Commercial Email Matters	Cyber Crime	01-Jan-04	Australia, United Kingdom of Great Britain and Northern Ireland, United States of America	Facilitate effective enforcement against spam violations; facilitate investigations of spam violations; assist one another in providing evidence that could assist in determining whether a person has committed a spam violation; law enforcement assistance	-	Government to Government
European Government CERT Group	Information Sharing, Research, Cyber Operations, Training		Sweden, Switzerland, United Kingdom of Great Britain and Northern Ireland, Finland, France, Germany, Netherlands, Norway	Jointly develop measures to deal with large-scale or regional network security incidents; Facilitate information sharing and technology exchange related to IT security incidents and malicious code threats and vulnerabilities; Identify areas of specialist knowledge and expertise that could be shared; Identify areas of collaborative research and development	-	CERT to CERT

Best Practices	2
Cyber Crime	12
Cyber Exercises	4
Cyber Operations	10
Information Sharing	9
Military	6
Policy	11
Research	10
Training	5
AGREEMENTS W/ DOUBLE-COUNTS	69

ANNEX 9 – India Agreements By Type

agreement_name	agreement_type	agreement_ date	agreement_signatories	agreement_summary	source	Combo53
India-Vietnam Bilateral Cooperation Agreements	Policy	01-Sep-16	Viet Nam, India	12 pacts in total, including defense, IT cooperation, space, and cybersecurity	Unsure of agreement type	Government to Government
Framework for the United States-India Cyber Relationship	Cyber Crime, Information Sharing, Research, Best Practices, Cyber Exercises, Training	01-Jun-16	United States of America, India	Sharing best practices, sharing information on a real time or near real time basis, R&D, combat cyber crime, joint training programs, facilitating joint tabletop exercises.	-	Government to Government
Joint Statement between India and Thailand	Cyber Crime	01-Jun-16	Thailand, India	Ramp up cooperation in cybersecurity; welcomed the initiative for the training of Thai officers by India's Central Bureau of Investigation in cyber crime investigation and computer forensics.	-	Government to Government
India-UAE Bilateral Cooperation Agreements	Cyber Crime, Information Sharing	01-Feb-16	United Arab Emirates, India	7 agreements including cybersecurity, pact on cyber space for greater synergy between security agencies to combat efforts to radicalize youths through online platforms; coordination and exchange of information in cyber crime; training in cyber crime investigation	-	Government to Government

MoU with India and Papua New Guinea for Establishing a Center of Excellence in IT	Research	01-Jan-16	India, Papua New Guinea	Unsure if the agreement includes cyber components; text not found	-	Government to Government
Joint Statement between the Indian Ministry of Home Affairs and the Ministry of Public Security for the People's Republic of China	Cyber Crime	21-Nov-15	China, India	Strengthen cooperation on cyber crime including telecom fraud, exchange visits, and cooperation in law enforcement capacity building.	-	Government to Government
Joint Statement between India and the UK	Cyber Crime, Training	01-Nov-15	United Kingdom of Great Britain and Northern Ireland, India	Work together to educate and train cybersecurity professionals; expand the UK's Cheyening Cyber Scholarships program for India; establish a cybersecurity training center of excellence; UK will provide advice on setting up the Indian Cyber Crime Coordination Center; Early conclusion of an MoU on CERT to CERT cooperation	-	Government to Government
Joint Statement: 2015 United States-India 4th Cyber Dialogue	Cyber Crime, Research	11-Aug-15	United States of America, India	Increased collaboration on cybersecurity capacity-building, cybersecurity R&D, and in combatting cyber crime.	-	Government to Government
MoU between Codenomicon Defensics and India's Gujarat Forensics University	Cyber Crime, Research, Training	13-Jan-15	Finland, India	Collaborate on cybersecurity research and development; GFSU CyberLab will conduct research, development, training, and services in vulnerability testing ana analysis, cyber incident monitoring, and computer forensics	-	Industry to Industry

Agreement between CERT India and Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)	Cyber Operations	01-Jan-15	India, Japan	Combat spam, detect symptoms and quick response to cyber attacks	-	CERT to CERT
India-Russian Cooperation	Cyber Crime, Information Sharing, Training	01-Jan-15	India, Russian Federation	Set up an expert group on cybersecurity and counterterrorism; exchange of information and cooperation monitoring ISIL activity in cyber realm (Jihadi chat and online recruitment)	-	Government to Government
India-Uzbekistan Pact to Boost Cooperation	Information Sharing	01-Jan-15	Uzbekistan, India	Expand cooperation in cybersecurity	-	Government to Government
MoU between Cybersecurity Agency (CSA - Singapore) and the Department of Electronics and Information Technology of India	Information Sharing, Best Practices	01-Jan-15	Singapore, India	Establish framework for professional dialogue; cooperation among CERTs for operational readiness and response; collaboration related to smart technologies; exchange of best practices; human resource development	-	Agency to Agency
MoU between Cybersecurity Malaysia and CERT India (CERT-In)	Cyber Crime, Information Sharing, Cyber Operations, Best Practices	01-Jan-15	India, Malaysia	Cooperation and exchange of information regarding cybersecurity incident managenent, technology cooperation, cyberattacks, policies, best practices, and mutual response to cybersecurity incidents	-	Agency to CERT

MoU between Indian Ministry of Communications and IT and the Department of Public Safety and Emergency Preparedness of Canada	Information Sharing, Cyber Operations	01-Jan-15	Canada, India	Cooperation in cybersecurity (no specific details mentioned)	-	Agency to Agency
Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security	Policy	02-Jul-14	Australia, Singapore, Spain , Sweden, Turkey, United Kingdom of Great Britain and Northern Ireland, United States of America, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, Pakistan, Republic of Korea	IT products and protection profiles that earn a Common Criteria Certificate, based on a collaborative Protection Profile (cPP) and Evaluation Assurance Levels, can be procured and used without further evaluation.	-	Government to Government
MoU between Cert-In and Korea Internet and Security Agency (KISA)	Information Sharing	16-Jan-14	India, Republic of Korea	Launched a cyber affairs dialogue for regular interaction to enhance information and knowledge sharing, expert exchanges, etc.	-	Agency to Agency
Agreement between India and Japan to Cooperate in the Fields of Cybersecurity and Green Information and Communications Technology (ICT)	Research, Cyber Operations, Training	01-Jan-14	India, Japan	Combat spam project; project for detecting symptoms and quick response to cyberattacks	http://pib.nic.in/newsite/PrintRelease.aspx?relid=112548	Government to Government

Druzhba-Dosti: A Vision for Strengthening the Indian-Russian Partnership over the Next Decade- Joint Statement	Policy, Cyber Operations	01-Jan-14	India, Russian Federation	Collaborate to promote safe, secure, and sustainable use of ICTs (information and communication technology) globally	http://pib.nic.in/newsite/PrintRelease.aspx?relid=113166	Government to Government
India-Australia Joint Declaration on Security Cooperation	Policy, Cyber Operations	01-Jan-14	Australia, India	Exchanges on cyber policy and cooperation between CERT India and CERT Australia	http://india.embassy.gov.au/ndli/pa5009jsb.html	CERT to CERT
MoU between Korea Computer Emergency Response Team Coordination Center (KRCERT/CC) and CERT India, DeitY in the field of Cybersecurity	Information Sharing	01-Jan-14	India, Republic of Korea	Promote cooperation and exchange of information on cybersecurity	-	CERT to CERT
UK Cyber Crime deal with India	Cyber Crime, Information Sharing, Training	19-Feb-13	United Kingdom of Great Britain and Northern Ireland, India	India to be Britain's "trusted partner" over cyber crime and security; Create a joint task force to exchange and share information about identifying and countering threats; Police training exchanges in cyber forensics and other areas of detection and enforcement; Regular cooperation meetings between leaders in cybersecurity research from academia and industry	-	Government to Government

Five Initiatives for Strengthening the India-Indonesia Strategic Partnership	Information Sharing, Cyber Operations	01-Jan-13	India, Indonesia	Enhance cooperation on cyber crime and cybersecurity issues	http://mea.gov.in/bilateral-documents.htm?dtl/22318	Government to Government
MoU between the United States and India	Information Sharing, Best Practices	19-Jan-11	United States of America, India	Promote closer cooperation and timely exchange of information; promote best practices for the exchange of critical cybersecurity information and expertise between the two governments through the Indian Computer Emergency Response Team (CERT-In), Department of Information Technology, Ministry of Communications and Information Technology, and DHS' United States Computer Emergency Readiness Team (US-CERT).	-	Government to Government
Joint Action Plan for Furthering the Strategic Partnership between the Republic of India and the Republic of Kazakhstan (Road Map) for the period of 2011-2014	Information Sharing	01-Jan-11	India, Kazakhstan	Bilateral cooperation and projects on topics to include cybersecurity	-	Government to Government

MoU between CERT-In (India), Department of Information Technology of India and Kz-CERT (Kazakhstan)	Information Sharing, Policy, Cyber Operations	01-Jan-11	India, Kazakhstan	Development of cooperation in the area of Information Security and covers the scope of mutual response to cybersecurity incidents, exchange of information on spam and other cyber-attacks, exchange of information on prevalent cybersecurity policies and exchange of human resources	-	CERT to CERT
US-India Cybersecurity Forum (2006)	Information Sharing	01-Jan-06	United States of America, India	Added cooperation in transportation and financial sectors; set up an India Information Sharing and Analysis Center and the India Anti-Bot Alliance	-	Government to Government
US-India Cybersecurity Forum (2004)	Cyber Crime, Research, Cyber Operations, Military	01-Jan-04	United States of America, India	Established five joint working groups to cover legal cooperation and law enforcement, research and development, critical information infrastructure, watch and warning emergency response, defense cooperation, and standards and software assurance.	-	Government to Government
US-India Cybersecurity Forum (2001)	Information Sharing, Cyber Operations	01-Jan-01	United States of America, India	CERT-In and US National Cybersecurity Division share expertise in artifact analysis, network traffic analysis, and exchange of information; US-India High Technology Cooperation Group formed in 2002	-	Government to Government

29 TOTAL AGREEMENTS	
Best Practices	4
Cyber Crime	11
Cyber Exercises	1
Cyber Operations	10
Information Sharing	16
Military	1
Policy	4
Research	6
Training	6
AGREEMENTS W/ DOUBLE-COUNTS**	59