COMPARING AND CONTRASTING SPACE AND CYBER GOVERNANCE IN MULTILATERAL FORUMS AND U.S. POLICY INITIATIVES

Erica Symonds
University of Maryland – School of Public Policy
Policy Engagement Project, May 2019
Client: Secure World Foundation

Table of Contents

Executive Summary

Over the past decade, governance initiatives focused on the space and cyber domains have worked to develop norms, guidelines, and other types of rules with mixed success. This project compares and contrasts space and cyber governance work, both in multilateral forums and in U.S. policy, over the past decade. It considers governance initiatives through two frameworks, one for multilateral forums and one for national policy in the United States. The framework for multilateral forums focuses on the time frame, types of participants, goals or purpose, outcome, use of soft or hard law, and level of success. The framework for U.S. policy considers the policy type, release date, drivers or motivations, mentions of the commercial sector or commercial interests, inclusion of arms control issues, inclusion of "global commons" issues, and overlap between space and cyber issues. These frameworks allow for comparisons of key characteristics of the initiatives in order to determine implications for future space and cyber governance efforts.

At the international level, both space and cyber governance have taken place at the United Nations, in regional forums, and in organizations incorporating private companies, experts, and academics. More efforts over the past decade have been focused on creating soft law. Both the United Nations and European Union have worked on space and cyber governance. Challenges at the UN include states blocking consensus and struggling to fundamentally agree on a path forward. In the past decade, states have more often created new forums around cyber issues than space issues, and regional organizations have more often focused on cyber issues.

In the United States, the release of cyber policies has been more spread out over the past decade, while space policies have been more concentrated within the past few years since the National Space Council was reestablished. A number of domestic space and cyber policies were issued as updates to policies from previous administrators. In both space and cyber policies, references to the commercial sector have been common, while there has been little to no mention of arms control or global commons issues. Only one initiative of all domestic policies reviewed included an area of overlap between space and cyber issues.

For future initiatives, it is notable that governance efforts in the space and cyber domains are highly siloed, which may limit meaningful progress to reduce the chance of misunderstandings that could lead to conflict. Divisions among groups of states are also impeding progress at the UN. Cyber issues face challenges from opposing perspectives on how information in cyberspace and the internet should be governed, often split between Western and non-Western states. In space, this divide plays out as the United States tends to be at odds with Russia and China. The mixed success of space and cyber initiatives at the UN over the past decade raises questions about the effectiveness of consensus-based forums while regional organizations, multi-stakeholder forums, and domestic initiatives move forward. At the same time, the UN continues to play an important role by serving as a forum for states to negotiate and find areas of common ground when possible.

Introduction

This research project compares and contrasts cyber and space governance work in multilateral, international forums and in U.S. national policy over the past decade. The purpose of the project is to consider the characteristics of these governance initiatives and determine the implications for space and cyber governance efforts going forward. In particular, an examination of successful and ineffective aspects of governance initiatives could provide useful information for future governance efforts.

The project focuses on the past decade because cyber governance efforts began to receive greater attention and movement around 2008 to 2009. After President Obama took office in 2009, his administration released a number of new cyber policies and strategies. At the international level, experts began working on the Tallinn Manual focused on cyber warfare and international law in 2009, and the United Nations (UN) Group of Governmental Experts (GGE) focused on the cybersphere issued its first consensus report after meeting in 2009 and 2010.

Space governance has a much longer history than cyber governance and, unlike the cyber domain, a foundation of treaties upon which it can build. Becoming a player in cyberspace is much simpler than becoming a spacefaring nation. However, the space and cyber spheres share a number of similarities, particularly regarding the flow of information. Both are considered areas of emerging technology. They also face similar threats, and both are considered warfighting domains. The space and cyber realms are extremely interconnected, yet governance efforts at the national and international levels largely deal with each area separately. These silos may limit meaningful progress in multilateral forums engaged in important work to develop best practices, standards, transparency and confidence-building

measures (TCBMs), and other types of “rules of the road” that are needed to address areas of ambiguity and prevent misunderstandings that could provoke or escalate a conflict. The division between space and cyberspace could also become problematic from a national security perspective as threats to these domains become increasingly intertwined. Given the essential services provided by satellites and the magnitude to which the world relies on the internet and cyberspace, successful governance initiatives in the space and cyber domains can be highly beneficial to maintain security and stability to the greatest extent possible.

To enable comparisons of governance initiatives, I developed two frameworks, one for international efforts and another for domestic policy, to set parameters for how to examine particular characteristics of the initiatives. Through the frameworks, the initiatives can be analyzed based on particular facets and more easily compared across particular aspects. For this project, a multilateral governance initiative counts as a multi-stakeholder effort in an international forum, involving parties from multiple states (whether governments, nongovernmental organizations, companies, or other participants), that has received enough international attention to be discussed to some extent by experts, academics, or others offering commentary on the proceedings or outcome. The multilateral initiatives included typically aimed to produce some type of report or policy. Bilateral efforts were not included in the scope of this project due to the vast number that exist. U.S. governance initiatives included in the project consist of policy directives, strategies, or other forms of instruction from the executive branch. This does not include broader policies or strategies that might mention space or cyber but rather those that focus entirely on space or cyber. Furthermore, only the public, unclassified versions of documents were reviewed. The paper includes summaries of the

characteristics of interest for each initiative, not necessarily a summary of the content of the initiative or policy itself.

Multilateral Space and Cyber Governance

Framework for Comparison of International Governance Initiatives

The framework for comparing international governance initiatives in multilateral forums focuses on the time frame, types of participants, goals or purpose, outcome, use of soft or hard law, and level of success. This section explains the potential types of responses for each category.

Time Frame: The time frame is understood differently for different types of initiatives. It could indicate the period(s) of negotiations, or it could describe the time since a body was established. For example, the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security is broken down by the time frame of each session since five separate GGEs have already taken place with a sixth GGE starting in 2019.

Types of Participants: Some governance initiatives may involve a multi-stakeholder approach while others might be exclusively for member states. The types of participants in governance initiatives could be states, non-governmental organizations, private companies, technical experts, academics, or other types of organizations or individuals.

Goals or Purpose: The goals or the purpose of an initiative will be crucial to determine if it has been successful. A negotiating process, such as a UN GGE, may have specific goals it aims to meet, such as producing a consensus report, while other types of forums may have a specific purpose or mission.

Notable Outcomes: The outcomes of governance initiatives could vary widely. One type of outcome is a formal agreement. Another type of outcome could be an agreed upon set of measures or rules to follow voluntarily. The outcome of negotiations at UN bodies could be a consensus report. Outcomes could also include the implementation of measures. Alternatively, governance initiatives could fail to produce a concrete outcome.

Soft Law vs. Hard Law: Governance initiatives may produce soft law or hard law in the outcome of a process or negotiations. Soft law is voluntary, such as transparency and confidence building measures (TCBMs), best practices, standards, guidelines, or other types of "rules of the road." Hard law is legally binding, such as provisions in a treaty.

Level of Success: The level of success of a governance initiative is based on the goals or purpose of the initiative itself. This framework categorizes the level of success as "successful," "mixed success," or "unsuccessful." In determining success, there may be multiple factors to consider. If the goal of an initiative is to produce a consensus report or an agreement, achieving this would indicate one level of success. Another type of success, which may be challenging to determine, could be the implementation of an agreement or acceptance by more actors, such as a regionally-produced proposal being introduced at an international organization. The level of success may also be judged by commentary or expert opinions, as available.

Overview of Space Forums

Working Group on the Long-term Sustainability of Outer Space Activities, COPUOS, UN

The Committee on the Peaceful Uses of Outer Space (COPUOS) was created as a UN committee in 1959 to "govern the exploration and use of space for the benefit of all humanity: for peace, security and development."[1] In particular, COPUOS is known for its development of

the Outer Space Treaty and four other major space treaties. COPUOS oversees the Scientific and Technical Subcommittee and the Legal Subcommittee. It reports to the Fourth Committee of the General Assembly.[2] COPUOS has 92 Member States, and international organizations can hold observer status with COPUOS and its subcommittees.[3] COPUOS operates through consensus-based discussions, so an item will not receive formal approval if even one state votes against it. While this democratic process is valuable for developing accepted international norms, requiring consensus slows negotiations and sometimes halts progress, leading "many blame the requirement of consensus for the failure to develop any binding norms" since the initial five space treaties.[4]

In 2010, COPUOS formally created the Working Group on the Long-term Sustainability of Outer Space Activities, or the LTS Working Group, within the Scientific and Technical Subcommittee. It aimed to develop guidelines on the long-term sustainability of outer space activities, a type of soft law. The LTS Working Group included not only states in discussions but also "established and emerging space actors, private corporations, and civil society," an important aspect since any guidelines would impact the entire space community.[5] The forum successfully reached consensus on its first 12 LTS guidelines in June 2016[6] and on nine more guidelines and text for a preamble in February 2018.[7] In the summer of 2018, Russia blocked approval of a final report on the guidelines.[8] Nonetheless, the forum succeeded in developing 21 guidelines approved by consensus, which states have already begun to implement.[9]

Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, UN

The GGE on TCBMs in Outer Space Activities was established by the UN in 2011 to make recommendations in order to "improve international cooperation and reduce the risks of misunderstanding, mistrust, and miscalculations in outer space activities."[10] The GGE, along with other efforts such as the LTS Working Group, was seen as a way to get around the deadlock preventing progress in the UN Conference on Disarmament that focuses in part on space security issues. The GGE consisted of 15 international experts nominated by Member States and "expected to provide politically neutral expertise to the process."[11] The GGE held three different multi-day meetings from 2012 to 2013 and issued its final report, approved by consensus, in July 2013. Challenges following the GGE included getting states and international organizations to implement the recommended TCBMs.[12] Regardless, the GGE was "largely considered a success" and "remains the only time in the last two decades that the United States, Russia, and China all agreed on a space security-related resolution within the UN."[13]

Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space, UN

In 2017, the UN adopted a resolution co-sponsored by China and Russia to establish a GGE on "further practical measures for the prevention of an arms race in outer space." The GGE was created to consider and make recommendations on a legally-binding treaty focused on the prevention of an arms race in outer space (PAROS).[14] The GGE met in 2018 and 2019.[15] At its final meeting in March 2019, the GGE failed to adopt a final report, an objective that requires all participants to reach consensus.[16] States differed on how to approach PAROS, including

whether to pursue a legally-binding treaty or voluntary norms, and on the content of an international instrument.[17] Ultimately, states disagreed over the draft final report for the GGE because it included a wide variety of initiatives, leading the United States and others to each find different provisions that they opposed, rather than focusing on a narrower set of issues.[18]

Even though the United States participated in the GGE, it voted against the resolution creating the GGE at the UN Conference on Disarmament because the resolution focused on Russia and China's draft "Treaty on the Prevention of Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects" (PPWT) as "the foundation for the GGE's review."[19] The United States has "long opposed negotiating a legally-binding agreement based on the PPWT" because it does not address the problem of terrestrially-based anti-satellite (ASAT) weapons; "fails to resolve definitional problems of what constitutes a 'weapon in outer space,' given the dual-use nature of many space technologies"; and "fails to address the challenge of creating an effective verification regime," according to remarks by Ambassador Robert Wood.[20] Rather than implementing a legally-binding agreement, the United States preferred focusing on TCBMs for activities in outer space.[21]

International Code of Conduct for Space Activities, European Union

Member States of the European Union (EU) drafted an International Code of Conduct for Outer Space Activities in 2007 to 2008 as "one of the first exercises of the new powers to engage in foreign and security policy making given to the EU under the 2009 Lisbon Treaty."[22] The draft, which was in part a response to a 2006 UN General Assembly resolution asking states to develop proposals for space TCBMs, "skirted many thorny issues that have plagued prior international efforts to prevent an arms race in outer space."[23] The EU publicly released its

draft Code of Conduct in December 2008. It intended to use the draft agreement as a basis for negotiating a set of international voluntary "rules of the road" by incorporating feedback from non-EU countries and experts through consultative meetings that took place through 2013, resulting in several revised drafts.[24]

The most recent draft was issued in 2014, and the Code of Conduct has generally been declared dead. Efforts to present the Code of Conduct as a UN proposal failed to come to fruition, in part because it was drafted outside of UN processes and excluded non-EU members from the drafting process.[25] Russia and China apparently opposed the Code of Conduct because it failed "to make minimum space traffic standards purely technical and to limit the scope of the rules to civilian nongovernmental operations."[26]

Consortium for Execution of Rendezvous and Servicing Operations

The Consortium for Execution of Rendezvous and Servicing Operations (CONFERS), a project initially hosted and funded by the Defense Advanced Research Projects Agency (DARPA), is working to develop best practices for on-orbit satellite servicing (OOS) and rendezvous and proximity operations (RPO). CONFERS is a multi-stakeholder process incorporating experts from industry, academia, government, and the international community to develop "non-binding, consensus-derived technical and operational standards for RPO and OOS."[27] CONFERS began its work in 2018,[28] holding workshops in the United States and Germany to collaborate with industry partners and find areas for cooperation on development of standards.[29] In November 2018, CONFERS released its "Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS)."[30] In February 2019, it released an agreed upon set of "design and operational practices," which "are intended to

evolve based upon experience gained through future commercial and government servicing operations."[31] In the coming years, CONFERS plans to develop more technical standards and integrate them into existing international standards development organizations.[32] CONFERS' leadership and funding will also transition to the private sector.[33]

Other Noteworthy Initiatives

Manual on International Law Applicable to Military Uses of Outer Space

The Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS) Project "aims to develop a widely-accepted manual clarifying the fundamental rules applicable to the military use of outer space in times of peace and in periods of rising tension."[34] It launched in May 2016 and intended to complete the process within three years.[35] MILAMOS is being developed by an international group of subject-matter experts involved in areas of general international law, international space law, international humanitarian law, the law on the use of force, and "advanced technical aspects of space utilisation."[36]

MILAMOS was formed in part because of other non-governmental efforts that have successfully shaped state behavior, especially those focusing on the application of international law to "armed conflict in the emerging frontiers."[37] Examples include the Tallinn Manual on International Law Applicable to Cyber Warfare, San Remo Manual on International Law Applicable to Armed Conflict at Sea, and the Harvard Manual on International Law Applicable to Air and Missile Warfare. According to the MILAMOS website, these initiatives "demonstrate how international experts and engagement with governments can produce quasi-legal documents that enjoy widespread recognition and authoritativeness while avoiding many of the challenges inherent in multilateral negotiations between States on similar topics."[38]

Woomera Manual on the International Law of Military Space Operations

The Woomera Manual on the International Law of Military Space Operations is an international research project spearheaded by The University of Adelaide, The University of Exeter, the University of Nebraska and the University of New South Wales - Canberra, which are working to "develop a Manual that objectively articulates and clarifies existing international law applicable to military space operations."[39] The project, expected to be completed by 2020, "will draw on the knowledge of dozens of legal and space operations experts from around the world."[40] The Woomera Manual aims to replicate the success of the two versions of the Tallinn Manual on International Law Applicable to Cyber Operations, as well as other similar types of non-governmental efforts that "help clarify the application of the law governing resort to force and law of armed conflict to new domains and means and methods of armed conflict."[41] The project held its first workshop in the United States in February 2019.[42]

Overview of Cyber Forums

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

The UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security was first established in 2004 and has continued under six separate working groups so far. The most recent working group will meet from 2019 to 2021. Generally, the GGEs aim to recommend cooperative measures to strengthen information security at the global level and promote international cooperation in this field. The GGEs successfully produced consensus reports in 2010, 2013, and 2015 from the second, third, and fourth GGEs established. However, the groups did not reach consensus at the end of the first

GGE in 2005 or the fifth GGE in 2017. The GGEs have been recognized for "two major achievements: outlining the global cybersecurity agenda, and introducing the principle that international law applies to the digital space."[43]

In 2017, the GGE failed to reach consensus after three successful GGEs that advanced the development of norms and confidence-building measures for cyberspace. The GGE that met from 2016 to 2017 specifically focused on studying and how to address "existing and potential threats in the sphere of information security," as well as studying "how international law applies to the use of information and communications technologies by states," which proved to be a major point of contention.[44] The United States and other Western countries wanted to develop statements about how the use of information and communications technologies (ICTs) applies to different types of international law, such as humanitarian law, the right to self-defense, state responsibility, and countermeasures, while states including Russia and China argued that this could militarize cyberspace and instead wanted to focus on the peaceful settlement of disputes and conflict prevention.[45]

This disagreement is representative of what one expert describes as "a bipolar division in cyber security governance, reflecting two opposing political systems and sets of values."[46] One group includes the United States and European countries, and the second group includes Iran, Russia, China, and others. The differences between the groups "have been described as the cyber space element of a resurgent Cold War, in which neoliberal and democratic structures confront information control, authoritarianism, and rule-breaking."[47] While the GGEs have seen some notable success, it appears that this split will be problematic as cyber initiatives progress to more contentious matters.

Cyber Confidence-Building Measures, Organization for Security and Co-operation in Europe

The Organization for Security and Co-operation in Europe (OSCE) began working on cybersecurity in 2011 and formally decided to draft confidence-building measures (CBMs) in 2012 through the creation of an Informal Working Group under the OSCE's Security Committee. The OSCE subsequently adopted 11 CBMs in 2013 and five more CBMs in 2016.[48] Decisions are made by consensus at the OSCE.[49] As a regional security-focused organization with 57 participating states, it has taken "a more bottom-up approach" to developing norms for cybersecurity with a greater focus on "practical steps to improve cybersecurity cooperation and prevent misunderstanding and conflict."[50] While the OSCE's CBMs are voluntary, its language is stronger than that used by UN GGEs. The OSCE tends to use "will" and "shall" rather than "states should consider" and "states could."[51] Additionally, the OSCE is less transparent than UN bodies since it operates primarily in closed sessions.[52]

Directive on Security of Network and Information Systems, European Union

The EU adopted the Directive on Security of Network and Information Systems (NIS Directive), the first EU-wide, legally-binding legislation focused on cybersecurity, in 2016. It required EU Member States to transpose the NIS Directive into their own laws by May 2018. It aimed to improve Member States' preparedness, cooperation, and culture of security.[53] The NIS Directive was proposed in the European Commission in 2013.[54]

International Code of Conduct for Information Security, Shanghai Cooperation Organisation

The Shanghai Cooperation Organisation (SCO) provides a forum for members to explore consensus and cooperation on non-traditional security threats, initially focusing on terrorism, separatism, and extremism and later adding information security.[55] The SCO is an

intergovernmental international organization with eight members including China, Russia, India, and Pakistan, as well as four observer states and six dialogue partners.[56] It adopts decisions based on consensus.[57]

The SCO created an International Code of Conduct for Information Security that aims "to push forward the international debate on international norms on information security, and help forge an early consensus on this issue."[58] According to one analysis, "The Code is largely a product of regional norm-building undertaken within the SCO."[59] The SCO began addressing cybersecurity in 2007 by developing a "plan of action" for international information security. In 2009, the SCO agreed upon a formal convention for information security that defined basic concepts and identified top threats. The states used this convention to create an international code of conduct in 2011.[60]

The SCO submitted the Code to the UN General Assembly in 2011 and, after revision, again in 2015.[61] According to one expert, "China and Russia framed the promotion of the code as their contribution to the then nascent debate on the promotion of norms for state behavior in cyberspace," while the United States and other Western states "largely dismissed the code, arguing that it was an attempt … to justify greater state control [over] the Internet's governance structures and online content."[62] The revised Code proposed in 2015 appeared largely as an update to include new developments at the UN and seemed to "soften China and Russia's stance on states taking a leadership role on Internet governance issues."[63] It appeared "unlikely that the Russians and Chinese updated the code to make it more palatable to Western countries," such as by affirming that international law applies to cyberspace.[64]

World Conference on International Telecommunications, International Telecommunications Union

In December 2012, the International Telecommunications Union (ITU) held the World Conference on International Telecommunications (WCIT-12) to review the International Telecommunication Regulations (ITRs), "which serve as the binding global treaty designed to facilitate international interconnection and interoperability of information and communication services, as well as ensuring their efficiency and widespread public usefulness and availability."[65] The outcome of the conference was deemed highly controversial. The United States, United Kingdom, Canada, and other countries walked out of negotiations on the last day and did not sign the final document to revise the ITRs. The document, known as "Final Acts,"[66] revised legally-binding articles and added non-binding appendices. The United States and allies were particularly concerned by efforts by Russia, China, Iran, and others to gain "international legitimacy for practices that they already engage in—increased national control, surveillance, better attribution and identification of users, filtering," and more.[67] The 89 countries that signed the revised treaty must comply with it after domestic ratification, and the 80 countries that refused to sign "will continue to be bound by the original 1988 text" of the ITRs.[68] (Note: Since 151 countries attended, the numbers may have shifted.) One report stated that the lack of consensus meant that the "legitimacy of the revised treaty is on shaky ground."[69]

Global Commission on the Stability of Cyberspace

The Global Commission on the Stability of Cyberspace (GCSC) is a commission of experts that was established in 2017 to "develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in

cyberspace."[70] It has 27 Commissioners from various geographic regions and different sectors including government, industry, technical areas, and civil society, and its main partners include Microsoft Corporation and the governments of The Netherlands and Singapore.[71] The GCSC has issued a Call to Protect the Public Core of the Internet, a Call to Protect the Electoral Infrastructure, and Norm Package Singapore which includes "six new global norms for both state and non-state actors to help promote the peaceful use of cyberspace."[72]

Other Noteworthy Initiatives

Open-Ended Working Group, UN

In 2018, the UN approved a Russian-sponsored resolution to establish a new forum focused on cyber issues in 2019. It created an open-ended working group (OEWG) of the UN General Assembly "to study the existing norms contained in the previous UN GGE reports, identify new norms, and study the possibility of 'establishing regular institutional dialogue.'"[73] The OEWG will essentially compete with the GGE beginning in 2019, which was created through a resolution sponsored by the United States "to study how international law applies to state action in cyberspace and identify ways to promote compliance with existing cyber norms."[74] While GGEs have a smaller membership (usually 15-25 participants) and face a set timeline, OEWGs can include any of the 193 Member States of the UN and will exist until members decide to disband it.[75] Note that it is too soon to analyze the OEWG.

Tallinn Manuals/Cooperative Cyber Defense *Center of Excellence, NATO*

The North Atlantic Treaty Organization (NATO) facilitated the development of the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn 1.0) and the subsequent Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

NATO's Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn, Estonia, convened international legal experts to write the Tallinn Manuals. While Tallinn 1.0 writers were primarily law of armed conflict (LOAC) experts from the Western Hemisphere, CCDCOE gathered a broader group (in terms of areas of expertise and countries of origin to include countries such as Thailand, Japan, China, and Belarus) to write Tallinn 2.0. Other states and organizations attended as observers.[76] The manuals are meant to reflect the law and not a serve as a guide of best practices, and they are "policy and politics-neutral."[77] Tallinn 1.0 was written from 2009 to 2012 and released in 2013. A new group of experts convened in 2013 to expand the scope and wrote Tallinn 2.0, which was released in 2017. Tallinn 2.0 supersedes Tallinn 1.0.[78] Note that the Tallinn Manuals do not create new rules but rather aim to interpret existing law.

U.S. Space and Cyber Policy

Framework for Comparison of Domestic Policy Initiatives

The framework for U.S. domestic policy initiatives considers the policy type, release date, drivers or motivations, mentions of commercial sector or interests, inclusion of arms control issues, inclusion of "global commons" issues, and overlap between space and cyber matters. This section explains the potential types of responses for each category.

Policy Type: The type of policy refers to the entity overseeing the policy's development and releasing the policy. This could be White House or a government agency such as the Department of Defense, Department of State, Department of Homeland Security, etc.

Release Date: For U.S. policies, the time frame referenced refers to the date that the policy was publicly released or announced. This may be the specific date or the month and year.

Drivers or Motivations: Similar to identifying the goals or purpose of an international governance initiative, understanding the drivers or motivations of a domestic initiative could help shed light on why it was created and intentions around that initiative. If relevant, this could help indicate any impact of international initiatives on domestic policy.

Mention of Commercial Sector or Interests: Based on the text of the policy, it may be interesting to see if or how an initiative refers to the commercial sector or commercial interests. Both the space and cyber fields have experienced a rise in commercial sector participation in recent years, so the policies may correlate with these changes.

Arms Control Issues: Reviewing the text of a policy would indicate if there is any particular focus on arms control issues. It may be interesting to compare how space and cyber policies reference or aim to deal with arms control matters in these domains.

"Global Commons" Issues: Similarly, a review of the policy text would indicate if there is any reference to the nature of the space or cyber domain as a "global commons," meaning that is not controlled by any particular entity. It may be interesting to see if the government makes any outright references to the commons issue, especially considering that the U.S. government has at times tried to avoid describing the space and cyber domains in this way.

Overlap Between Space and Cyber: It appears that space policy and cyber policy have largely operated in silos. It would be notable if a space policy mentions cyber issues, or if a cyber policy mentions space issues, since the space-cyber overlap has received limited attention by the U.S. government and others involved in these areas.

Overview of Space Policies

National Space Policy of the United States

In June 2010, under President Obama, the White House released a new National Space Policy (NSP).[79] Among other areas, the policy focused on "energizing the privately funded space industry, expanding international space partnerships and sending manned missions farther into space."[80] The White House worked with "a couple of dozen departments," including "the State Department, the Joint Chiefs of Staff, and the Department of Energy, to develop a policy that "reflected the president's priorities."[81]

The NSP indicated the Obama administration's support for international cooperation in space and openness to an arms control treaty to limit space weapons, a sharp contrast to the Bush administration's policy and a return to the stance taken by previous administrations to focus on space arms control negotiations.[82] The NSP said the United States would pursue TCBMs for responsible and peaceful activities in space and "consider proposals and concepts for arms control measures if they are equitable, effectively verifiable, and enhance the national security of the United States and its allies."[83] The 2010 policy also differed from the Bush era policy by highlighting the commercial space sector, with a top goal to "energize domestic industries."[84] For instance, it directed federal agencies to "actively explore the use of inventive, nontraditional arrangements" such as "public-private partnerships, hosting government capabilities on commercial spacecraft," and buying "data products from commercial satellite operators."[85] The NSP touched on global commons issues by stating its intention to help preserve the space environment "for the responsible, peaceful, and safe use of all users," including through debris mitigation.[86] The NSP did not mention cyber issues.

National Security Space Strategy

In January 2011, the Department of Defense (DOD) and Office of the Director of National Intelligence released the unclassified summary of the first-ever National Security Space Strategy (NSSS). It notably described the space environment as "congested, contested, and competitive."[87] The document complemented the Obama administration's 2010 NSP. DOD viewed the NSSS as a "pragmatic approach to maintain the advantages derived from space while confronting the challenges of an evolving space strategic environment."[88] A space policy analyst described its broad "approach to security with an improved balance of commercial, civil, and military views of space," as well as its emphasis on international cooperation and use of "a multilayered approach to securing satellite capabilities, including norms and building resilience into U.S. space systems."[89]

The NSSS repeated the same statement as the 2010 NSP regarding the United States' willingness to consider arms control measures, in addition to its support for developing data standards, best practices, and TCBMs.[90] The NSSS also highlighted "energizing the U.S. space industrial base" as a part of the strategy to bolster national security.[91] Further similar to the NSP, the NSSS touched on global commons issues by stating that achieving its "objectives will mean not only that our military and intelligence communities can continue to use space for national security purposes, but that a community of nations is working toward creating a sustainable and peaceful space environment to benefit the world for years to come."[92] It also described space as "a domain that no nation owns but on which all rely."[93] The NSSS did not discuss cyber issues.

National Space Transportation Policy

On November 21, 2013, the White House released the National Space Transportation Policy,[94] an update to the Bush era 2004 policy. The new policy did not vary drastically from the 2004 version. New aspects included an emphasis on bolstering the commercial space transportation sector, such as by allowing new entrants to launch U.S. government payloads and encouraging "increased technological innovation and entrepreneurship."[95] The policy did not discuss arms control besides noting the need to conform with international arms control agreements.[96] It also did not touch on global commons or cyber issues.

National Space Weather Strategy

In October 2015, the White House released the National Space Weather Strategy, a product of the National Science and Technology Council. The strategy was developed by the Space Weather Operations, Research, and Mitigation (SWORM) task force, an interagency group established to "develop a national strategy and a national action plan to enhance national preparedness for space-weather events." The strategy highlighted the importance of international coordination and cooperation, but it did not focus on arms control, global commons, commercial sector, or cyber issues.[97]

NOAA Commercial Space Policy

In January 2016, the National Oceanic and Atmospheric Administration (NOAA), which is part of the Department of Commerce, released the NOAA Commercial Space Policy.[98] The policy was part of NOAA's push to procure weather data from the commercial space sector. According to the policy, NOAA sought "to leverage commercial space capabilities to capitalize on available extramural expertise, to improve weather forecasting, diversify NOAA's portfolio of

data collection capabilities, to promote U.S. space commerce and the industrial base, and to pursue enhancements in mission areas, program schedules, and costs."[99] In particular, NOAA was looking to work with the commercial sector regarding data buys, hosted payloads, rideshares, and launch services.[100] The policy did not focus on arms control, global commons, or cyber issues.

Presidential Executive Order -- Reviving the National Space Council

On June 30 2017, President Trump signed an executive order re-establishing the National Space Council "to provide a coordinated process for developing and monitoring the implementation of national space policy and strategy."[101] Among other things, the Council was directed to "foster close coordination, cooperation, and technology and information exchange among the civil, national security, and commercial space sectors."[102] The Council was last active in 1993 during the George H. W. Bush administration. The executive order also established a Users' Advisory Group, an entity meant to ensure that "the interests of industries and other non-Federal entities involved in space activities, including in particular commercial entities, are adequately represented in the Council."[103] The executive order did not focus on arms control, global commons, or cyber issues.

National Space Strategy

On March 23, 2018, the White House announced a new National Space Strategy focused on protecting "American interests in space through revised military space approaches and commercial regulatory reform."[104] The White House did not publicly release the strategy but rather a fact sheet about the strategy. The fact sheet noted, "The Trump administration's National Space Strategy prioritizes American interests first and foremost, ensuring a strategy

that will make America strong, competitive, and great."[105] It emphasized "peace through strength in the space domain" and highlighted four "pillars for a unified approach," one of which expressed support for the U.S. commercial sector and cooperation with international partners.[106] The strategy did not focus on arms control, global commons, or cyber issues.

Space Policy Directive -- Reinvigorating America's Human Space Exploration Program

On December 11, 2017, President Trump issued an executive order, "Reinvigorating America's Human Space Exploration Program," also known as Space Policy Directive-1 (SPD-1). It directed NASA to engage in greater space exploration. The policy noted, "the United States will lead the return of humans to the Moon for long-term exploration and utilization, followed by human missions to Mars and other destinations."[107] It did not touch on arms control, global commons, or cyber issues.

Space Policy Directive -- Streamlining Regulations on Commercial Use of Space

On May 24, 2018, President Trump signed SPD-2, instructing his administration to create new, streamlined regulations for the commercial space sector. The policy directed the Secretary of Transportation to create a new regulatory regime for launch and re-entry, including potentially requiring just a single license for all types of commercial space flight operations. SPD-2 also directed agencies to review commercial remote sensing, radio frequency spectrum, and export licensing regulations. The policy reorganized the Department of Commerce to consolidate its commercial space flight activities into one office.[108] SPD-2 stemmed from recommendations by the National Space Council and complaints from commercial space companies "feeling hampered by overly strict, complex, and lengthy U.S. government regulations."[109] It did not mention arms control, global commons, or cyber issues.

Space Policy Directive -- National Space Traffic Management Policy

On June 18, 2018, President Trump issued SPD-3, a national policy for space traffic management (STM). A major aspect of the directive is that it shifted responsibility for providing "the publicly releasable portion" of space situational awareness (SSA) data to satellite operators from DOD to the Department of Commerce. Beyond bolstering the sharing of U.S. government SSA data and STM services, it expressed support for "new opportunities for U.S. commercial and non-profit SSA data and STM services." The directive also focused on space debris mitigation, among other areas.[110] Like previous SPDs, SPD-3 came from recommendations by the National Space Council. It was also considered highly relevant for the global space community as the number of objects in space is expected to rapidly increase in the coming years,[111] but it did not focus specifically on global commons, arms control, or cyber issues.

Space Policy Directive -- Establishment of the United States Space Force

On February 19, 2019, President Trump signed SPD-4 to direct DOD to propose to Congress the creation of the United States Space Force "as a new armed service within the Department of the Air Force."[112] Under the proposal, the Space Force would "organize, train, and equip forces to provide for freedom of operation in, from, and to the space domain; to provide independent military options for national leadership; and to enhance the lethality and effectiveness of the Joint Force."[113] It would be led by a civilian Under Secretary of the Air Force for Space who would also serve as the Under Secretary for Space.[114] SPD-4 was considered a long-awaited formal action by the White House directing the creation of the Space Force. The Trump administration formally announced its intention to create a Space Force in August 2018.[115] SPD-4 did not discuss arms control, global commons, or cyber issues.

Overview of Cyber Policies

Cyberspace Policy Review

On May 29, 2009, the White House released the Cyberspace Policy Review following a presidentially-directed 60-day "clean-slate" review to "assess U.S. policies and structures for cybersecurity."[116] The review team consisted of government cybersecurity experts who "engaged and received input from a broad cross-section of industry, academia, the civil liberties and privacy communities, State governments, international partners, and the Legislative and Executive Branches."[117] The Cyberspace Policy Review "summarizes the review team's findings and outlines initial areas of action to help the United States achieve a more reliable, resilient, and trustworthy digital infrastructure for the future."[118] The review noted roles for the commercial sector, including "enterprise leadership responsibility," public-private partnerships for securing cyberspace, and innovation to address cybersecurity concerns.[119] It did not focus on arms control, global commons, or space issues.

International Strategy for Cyberspace

In May 2011, the White House released the International Strategy for Cyberspace.[120] The strategy "lays out the President's vision for the future of the Internet, and sets an agenda for partnering with other nations and peoples to achieve that vision."[121] It listed ideal norms for behavior for cyberspace and was meant to be "a strong foundation for the diverse activities we will carry out across our entire government."[122] The strategy noted the need to strengthen collaboration with the private sector.[123] It did not discuss arms control, global commons, or space issues.

DOD Strategy for Operating in Cyberspace

In July 2011, DOD released a Strategy for Operating in Cyberspace.[124] It was the first unified strategy for cyberspace ever released by DOD and "officially encapsulates a new way forward for DoD's military, intelligence and business operations."[125] The strategy included supporting technological innovation by businesses.[126] It did not focus on arms control, global commons, or space issues.

Presidential Executive Order -- Improving Critical Infrastructure Cybersecurity

On February 12, 2013, President Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." It touched on the private sector in regard to information sharing.[127] According to congressional testimony by Eric A. Fischer of the Congressional Research Service, the development of the executive order "involved a lengthy interagency process, with both agencies and stakeholders in the private sector providing input."[128] The executive order, together with Presidential Policy Directive-21 (described below), directed government efforts to protect critical infrastructure from cyber threats and "reinforce the need for holistic thinking about security and risk management."[129] It did not discuss arms control, global commons, or space issues.

Presidential Policy Directive -- Critical Infrastructure Security and Resilience

On February 12, 2013, the same day that President Obama signed Executive Order 13636, the White House also released Presidential Policy Directive-21 (PPD-21), "Critical Infrastructure Security and Resilience." PPD-21 was an effort to advance "a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."[130] It set "national policy on critical infrastructure security and resilience."[131] The directive required

that government agencies work with industry and private sector stakeholders.[132] It did not discuss arms control, global commons, or space issues.

NIST Framework for Improving Critical Infrastructure Cybersecurity

On February 12, 2014, the National Institute of Standards and Technology (NIST), which is part of the Department of Commerce, released the Framework for Improving Critical Infrastructure Cybersecurity.[133] NIST created the Framework based on Executive Order 13636 which called for developing "a voluntary risk-based Cybersecurity Framework – a set of industry standards and best practices to help organizations manage cybersecurity risks."[134] The NIST Framework, developed with collaboration between the government and private sector, "uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."[135] On April 16, 2018, NIST released an updated Framework (Version 1.1) that "refines, clarifies, and enhances Version 1.0."[136] Neither versions of the Framework focused on arms control, global commons, or space issues.

DOD Cyber Strategy (2015)

In April 2015, DOD released a new Cyber Strategy.[137] Its purpose was "to guide the development of DoD's cyber forces and strengthen our cyber defense and cyber deterrence posture" and set "objectives for the Department to achieve over the next five years and beyond."[138] It mentioned the importance of working with the private sector, among other types of actors, to "strengthen deterrence by denial through improved cybersecurity."[139] It also focused on building the cyber workforce, in part by implementing "private sector exchange programs."[140] While the strategy did not specifically discuss arms control, it did focus on

countering the proliferation of destructive malware through international regimes and best practices, as well as domestic export control regimes for dual-use technologies.[141]

The Cyber Strategy was an update to the strategy released in 2011. The 2015 version was much more comprehensive and detailed, including about "DOD's role in defending the United States against cyber attacks" and "how DOD will integrate cyber capabilities into military operations."[142] It was also meant to provide guidance for DOD's Cyber Mission Force structure. The new strategy was an effort by DOD "to be more transparent about U.S. military doctrine, policy, roles, and missions in cyberspace, both to better inform the public debate and expand declaratory policy for cyber conflict."[143] It was a major change from the 2011 strategy that "made little reference to the Pentagon's operational or offensive cyber capabilities."[144]

Cybersecurity National Action Plan

On February 9, 2016, the White House released a fact sheet of the Cybersecurity National Action Plan. President Obama directed his administration to implement a Cybersecurity National Action Plan, which was "the capstone" of more than seven years of work by the Obama administration, "building upon lessons learned from cybersecurity trends, threats, and intrusions."[145] The plan aimed to improve "cybersecurity across the Federal Government, the private sector, and our personal lives."[146] As part of the plan, the government intended to work with "top strategic, business, and technical thinkers from outside of government to study and report on what more we can do to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security."[147] The plan did not discuss arms control, global commons, or space issues.

Department of State International Cyberspace Policy Strategy

In March 2016, the Department of State released its International Cyberspace Policy Strategy, a report submitted to Congress to provide an update on the implementation of President Obama's International Strategy for Cyberspace.[148] It did not focus on the commercial sector, arms control, global commons, or space issues.

Presidential Executive Order -- Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

On May 11, 2017, President Trump signed an executive order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." It focused on addressing cybersecurity concerns in the executive branch.[149] It also built upon President Obama's Executive Order 13636, "Improving Critical Infrastructure Security," including by supporting private sector owners and operators of critical infrastructure.[150] It did not discuss arms control, global commons, or space issues.

DOD Cyber Strategy (2018)

In September 2018, DOD released a summary of its new Cyber Strategy,[151] replacing the strategy released in 2015. Its purpose was to explain how DOD "will implement the priorities of the National Defense Strategy in and through cyberspace."[152] The strategy aimed to expand "cyber cooperation with allies, partners, and private sector entities."[153] It did not focus on arms control, global commons, or space issues.

National Cyber Strategy

In September 2018, the White House released the National Cyber Strategy.[154] It replaced the previous cyber strategy from 2003 and provided updated priorities for

government agencies.[155] The new strategy notably included a brief section on improving cybersecurity in space as part of its agenda to bolster critical infrastructure. It stated:

> "The United States considers unfettered access to and freedom to operate in space vital to advancing the security, economic prosperity, and scientific knowledge of the Nation. The Administration is concerned about the growing cyber-related threats to space assets and supporting infrastructure because these assets are critical to functions such as positioning, navigation, and timing (PNT); intelligence, surveillance, and reconnaissance (ISR); satellite communications; and weather monitoring. The Administration will enhance efforts to protect our space assets and support infrastructure from evolving cyber threats, and we will work with industry and international partners to strengthen the cyber resilience of existing and future space systems."[156]

The strategy also touched on protecting American businesses from malicious actors, as well as partnering with the private sector to improve cybersecurity, including specifically for risk management and incident response related to critical infrastructure.[157] The strategy did not delve into arms control or global commons issues.

Comparisons and Findings

International Governance Initiatives in Multilateral Forums

A number of similarities exist between international governance initiatives focused on space and cyber issues. There is no primary entity that governs either area. Rather, a mix of initiatives at the international and regional levels have taken place over the past decade. Notably, both the United Nations and European Union have been working on space and cyber

governance. More efforts over the past decade have been focused on creating soft law. At the UN, there have been multiple GGEs for space and cyber, although GGEs have more consistently been created for cyber issues. Three cyber GGEs successfully reached consensus on a final report, while only one space GGE did so. The space-focused forums at the UN have faced challenges in part due to single countries blocking consensus, as happened with Russia on the final report for the COPUOS LTS guidelines.

Looking at the past decade, states have been more interested in creating new forums to discuss and develop rules of some kind about cyber issues than space issues. More regional organizations are focusing on cyber than space. Interestingly, the cyber GGE process now faces competition from the newly created open-ended working group (OEWG) at the UN, which will allow participation from more states. While this could be beneficial for greater inclusion, it could also make it more difficult to reach consensus. Some have expressed concern that the OEWG will split attention on cyber issues and allow "forum shopping."[158] States have made proposals for other types of forums to discuss cyber issues, as well. They have proposed creating a COPUOS-like committee for cyber, essentially a cyber committee of the General Assembly, given the productive track record of COPUOS in developing international agreements through its history. However, the United States would likely oppose such a committee for cyberspace since officials are "less interested in creating new norms as they are enforcing those that are already on the books" and would rather "work with like-minded states to call out norm violating behavior and impose costs on those who don't play by the rules."[159]

Another point where space and cyber governance differ is the way states are divided on major issues. In space efforts such as the GGE on PAROS, it is clear that countries such as Russia

and China want to create a legally-binding international document around weapons in space while the United States would rather focus on norms and TCBMs. While more and more states are becoming players in space, the top spacefaring nations are still the lead players. In the cybersphere, however, many more countries have critical stakes in international rules and want to be involved in developing those rules. The divide between states on cyber issues is typically portrayed as Western versus non-Western. Non-Western states such as China, Russia, and Iran want to exert national control over content in cyberspace, while Western states including the United States and European countries seek "an open and free internet driven largely by global market competition with some government regulation and civil society observation."[160] This split is apparent through the splintering of cyber efforts at the UN with the creation of the OEWG alongside the GGE process. At the same time, the OSCE, whose membership includes Western countries and Russia, successfully agreed upon norms for cybersecurity cooperation.

Regional organizations have taken on a notable role in developing governance initiatives. The EU and the Shanghai Cooperation Organisation each crafted a code of conduct, the EU for space and the SCO for cyber, to lay out norms in line with the views of their members. While successful internally, each organization has tried and failed to gain traction at the UN with their proposed codes of conduct. It appears that these organizations have not been able to gain broader international acceptance of the codes of conduct because they were drafted outside of UN processes and only reflect the viewpoints of the limited number of participants involved. Related to this, regional organizations such as the SCO and the OSCE operate with greater secrecy, so the lack of transparency about how governance initiatives develop and how members reach agreement may hinder further international progress.

Alongside multilateral forums with states as the primary actors, other initiatives have formed to interpret international law as it relates to both space and cyber. The Tallinn Manual focused on cyber operations was the first of these, and two space-focused efforts, the Woomera Manual and MILAMOS, followed in more recent years in part due to the success of the Tallinn Manual. These efforts allow academics and experts outside of government to participate in "a multilateral norm-building effort even if it only includes members of one alliance system," as in the case of the Tallinn Manual under the auspices of NATO.[161] Even if these manuals are initially developed only for a limited number of states, they can still play a role in elucidating how international law is relevant for these domains. Private industry is also working to develop norms and guidelines, as seen with CONFERS for space operations and the Microsoft-backed Global Commission on the Stability of Cyberspace.

Domestic Policy Initiatives in the United States

Over the past decade, the United States has released a number of strategies and policies dictating approaches to address space and cyber issues. The White House was the top issuer of national policy for both space and cyber. However, cyber policy initiatives came from a broader group of agencies as a whole, including DOD, NIST, and the State Department. Additionally, the release of cyber policies was more spread out over the past decade, while space policies were more concentrated within the past few years since the National Space Council was revived.

Comparing publicly released initiatives, the Obama administration issued more policies focused on cyber than space, while the Trump administration issued more policies focused on space than cyber. A number of domestic space and cyber policies were issued as updates to policies from previous administrators to align with new viewpoints or keep current with

changes in these domains. Although it was not specifically mentioned, the Office of Personnel Management hack and other high-profile cyberattacks on U.S. companies may have served as an impetus to develop domestic cyber policies.

In both space and cyber, references to the commercial sector or commercial interests have been common in national policies and strategies. This is unsurprising given the increasing involvement of industry actors in both sectors. None of the cyber policies over the past decade referenced arms control or global commons issues, while two space strategies did so early on in President Obama's tenure. Only one initiative of all domestic policies reviewed, the National Cyber Strategy released in 2018, included an area of overlap between space and cyber issues.

Another noteworthy aspect of cyber policy is that the Trump administration has used more aggressive language around cyber issues. In the DOD Cyber Strategy released in 2018, an update to the 2015 policy, DOD placed a much greater focus on offensive activities with more forceful language around deterring and defending against cyberattacks. On a related note, the 2018 Nuclear Posture Review suggests that the United States could consider using a nuclear weapon in response to a cyberattack, although ambiguity around the policy exists.[162]

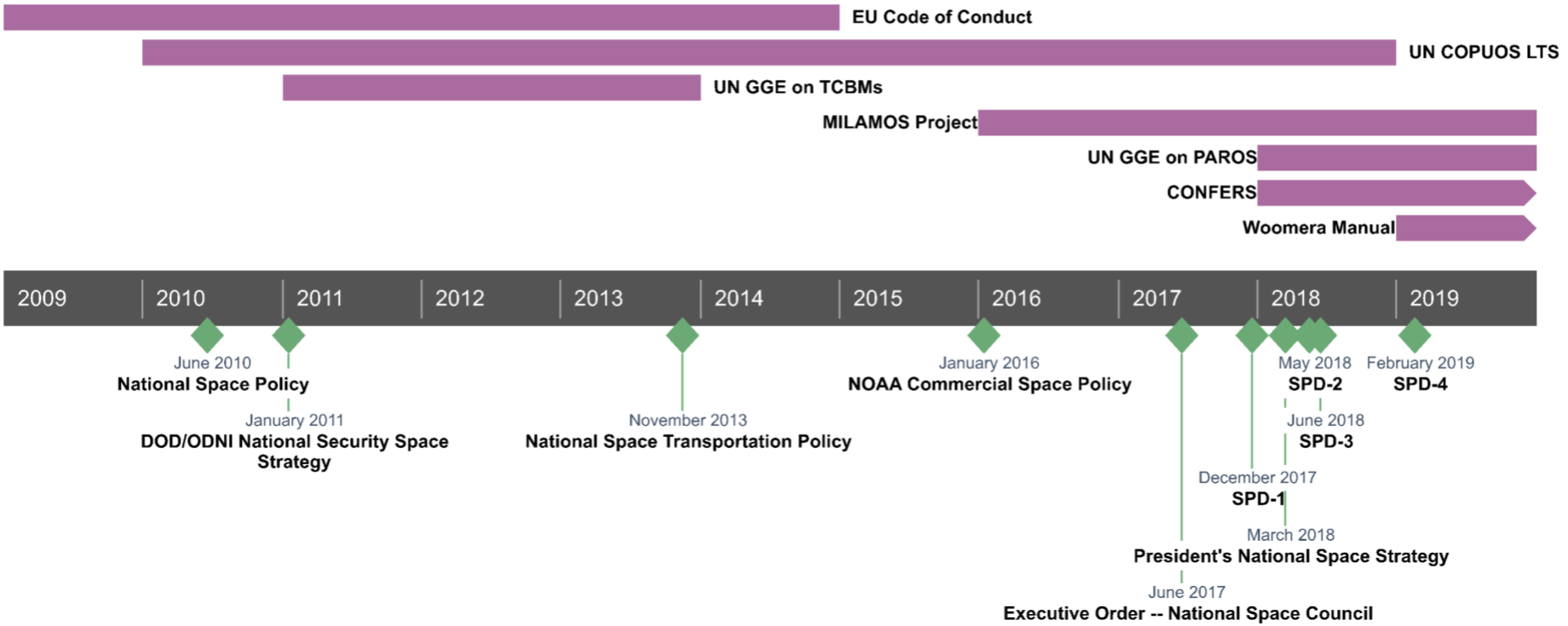
U.S. policies on cyber and space also tie into multilateral efforts. In the cybersphere, the United States has placed a significant focus on protecting critical infrastructure and bolstering government agencies against cyberattacks. This aligns with the types of norms that it has been pushing, along with Western allies, at the UN. Regarding space, the United States has been developing policies to support the space industry, including by improving licensing processes and other regulations. The government is working to develop better management systems for SSA and STM to provide greater protection for satellites in space, an issue with global

implications since the United States provides SSA services for 100 other countries, companies, and organizations.[163] Furthermore, the Trump administration's efforts to develop a U.S. Space Force as a new military branch reflect its desire to protect against adversaries with ground-based and on-orbit ASAT weapons. This relates to the challenges facing multilateral forums focused on space issues given the obstacles around even defining a weapon in space or reaching agreement on how to further develop norms against their use, an issue that recently received renewed attention following India's ASAT test.[164]

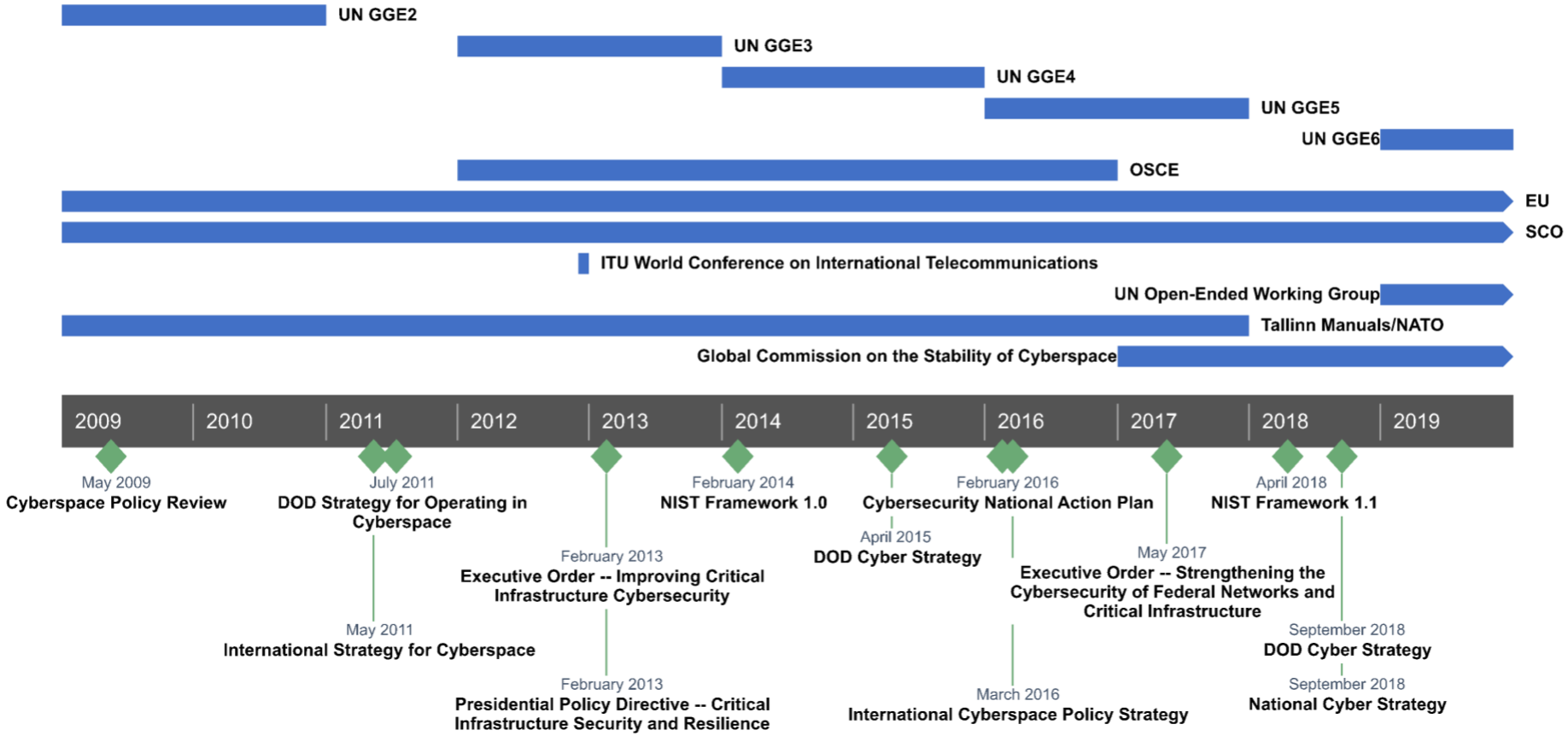
Timelines

Based on the initiatives and policies reviewed, I created two timelines to show how multilateral governance initiatives align with U.S. policy initiatives over the past decade. The space governance timeline shows that efforts are more concentrated on recent years, while the cyber governance timeline indicates that efforts have been more consistently spread out over the past decade.

Space Governance Timeline



Cyber Governance Timeline



Implications for Future Governance Initiatives

The way that governance initiatives focused on space and cyber have been so deeply siloed may be problematic moving forward. Cybersecurity of space assets and infrastructure is an area that has received some attention in the academic and think tank community, but it may take leadership from the private sector to make progress in this area. Encouragingly, the U.S. government and space industry are working together to develop the first Information Sharing and Analysis Center (ISAC) for space. The U.S. government has created ISACs for other industries, such as aviation, financial services, and energy, since the late 1990s "to collect, analyze and disseminate information about security threats that affect specific sectors."[165] The creation of the Space ISAC supports the National Cyber Strategy, released by the White House in September 2018, which directs the government to work with private industry to "strengthen the cyber resilience of existing and future space systems."[166]

Divisions among groups of states are impeding progress on governance issues at the UN. For instance, Western and non-Western states traditionally take opposing views on certain cyber issues. Western states intend to develop norms focused "on protecting the Internet's global infrastructure and operations rather than on governments' control over what their own citizens can see," although they support some controls on content such as "using online media to spread fake news or manipulate public opinion right before an election."[167] Non-Western states focus "on the political effect of information and the belief that content is used against states to destabilize their regimes," and, consequently, want "greater recognition of sovereign rights in cyberspace."[168] Non-Western states seek a treaty with "a more state-centric model for Internet governance," which would "upend the Western insistence on freedom of information

as a basic human right" and "contradict the West's preference for multi-stakeholder governance in the cybersphere."[169] It is notable, however, that not all states fit into this dichotomy. For instance, Egypt and the Gulf states cooperate closely and want to maintain a positive relationship with Western allies, yet they have taken a more authoritarian approach to national cyber issues.[170]

Although this project does not focus on bilateral efforts, the U.S.-China Cyber Agreement of 2015 is a significant example of agreement between states on different sides of the cyber divide. The two countries agreed not to hack each other's private companies to steal trade secrets that would benefit domestic businesses. Analyses by two digital security firms found that "Chinese-backed cyber theft of American trade secrets" dropped about 90 percent within the first two years of the accord, greatly reducing the estimated hundreds of billions of dollars that the theft previously cost the United States each year.[171] Although the agreement appeared initially successful, analysts pointed out that China may simply have shifted its hacking targets to other states.[172] Furthermore, in 2018, a U.S. government official accused China of violating the agreement.[173] Even so, the fact that the two states could reach agreement in one area of cyberspace is notable for future governance initiatives.

At the UN, the mixed success of space and cyber initiatives over the past decade raises questions about the effectiveness of consensus-based forums. In both domains, regional organizations and multi-stakeholder forums consisting of non-governmental organizations, private companies, and subject matter experts have moved forward with efforts to develop norms and rules. The United States and other governments have also engaged in unilateral efforts to form policies that could become more widely understood as norms. While it may be

easier to achieve agreement domestically, regionally, or among experts and private industry, successful global norms require the buy-in of a significant number of states and other key stakeholders, as seen with the unsuccessful efforts by the EU and SCO to elevate their proposed codes of conduct to the international level. This makes the UN ideal for governance forums given its large membership. As the UN continues to serve as a place for states to negotiate and find areas of common ground, states and other actors can also work toward overcoming divisive issues in forums driven by industry, academics, and smaller groups of states. It remains to be seen whether other types of multilateral forums and domestic initiatives can have a greater international impact than the UN as the cyber and space domains continue to evolve.

---

[1] United Nations Office for Outer Space Activities, "Committee on the Peaceful Uses of Outer Space," accessed February 28, 2019, http://www.unoosa.org/oosa/en/ourwork/copuos/index.html.
[2] Ibid.
[3] United Nations Office for Outer Space Activities, "COPUOS History," accessed February 28, 2019, http://www.unoosa.org/oosa/en/ourwork/copuos/history.html. United Nations Office for Outer Space Activities, "Committee on the Peaceful Uses of Outer Space: Membership Evolution," accessed February 28, 2019, http://www.unoosa.org/oosa/en/ourwork/copuos/members/evolution.html.
[4] R.S. Jakhu and J.N. Pelton (eds.), "Overview of the Existing Mechanisms of Global Space Governance," Chapter 2 in *Global Space Governance: An International Study*, Springer International Publishing (2017): 32.
[5] Christopher D. Johnson and Victoria Samson, "A summer update on the COPUOS long-term sustainability guidelines," *The Space Review*, July 24, 2017, http://www.thespacereview.com/article/3291/1.
[6] Ibid.
[7] Josh Wolny, "The UN COPUOS Guidelines on the Long-term Sustainability of Outer Space Activities," Secure World Foundation, Updated August 2018, https://swfound.org/media/206227/swf_un_copuos_lts_guidelines_fact_sheet_august_2018.pdf.
[8] Theresa Hitchens, "Forwarding Multilateral Space Governance: Next Steps for the International Community," CISSM Working Paper, August 2018, http://cissm.umd.edu/sites/default/files/ForwardingMultilateralSpaceGovernance%20updated82018.pdf.
[9] Secure World Foundation, "SWF Highlights Implementation of Sustainability Guidelines and Commercial Satellite Servicing Standards at UN," February 18, 2019, https://swfound.org/news/all-news/2019/02/swf-highlights-implementation-of-sustainability-guidelines-and-commercial-satellite-servicing-standards-at-un.
[10] Christopher Johnson, "The UN Group of Governmental Experts on Space TCBMs," Secure World Foundation, Updated April 2014, https://swfound.org/media/109311/swf_gge_on_space_tcbms_fact_sheet_april_2014.pdf.
[11] Ibid.
[12] Ibid.

[13] Brian Weeden, "Testimony before the U.S.-China Economic and Security Review Commission," Hearing on "China in Space: A Strategic Competition?" April 25, 2019, 14, https://swfound.org/media/206425/weeden_uscc_testimony_april2019.pdf.
[14] UN Disarmament Commission, "2018 United Nations Disarmament Commission," Non-paper by the Secretariat (Working Group II), https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/03/WG2-secretariat-non-paper-outer-space-TCBMs-FINAL.pdf.
[15] Daniel Porras, "Brief of UN Space Security Dialogues" in "Space Alert," Volume VI, Issue 4, Observer Research Foundation, November 1, 2018, https://www.orfonline.org/research/space-alert-volume-vi-issue-4-45315/.
[16] Weeden, "Testimony before the U.S.-China Economic and Security Review Commission," 15.
[17] UN Disarmament Commission, "Recommendations to promote the practical implementation of transparency and confidence-building measures in outer space activities with the goal of preventing an arms race in outer space, in accordance with the recommendations set out in the report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities," Working paper submitted by Nigeria (on behalf of the African Group), A/CN.10/2019/WP.1, April 25, 2019, https://undocs.org/A/CN.10/2019/WP.1. See paragraphs 7, 25, 26, and 51.
[18] Brian Weeden, feedback to author, April 29, 2019.
[19] Ambassador Robert Wood, "Explanation of Vote in the First Committee on Resolution L.54: Further Practical Measures for the Prevention of an Arms Race in Outer Space," United States Mission to the United Nations, October 20, 2017, https://usun.state.gov/remarks/8085.
[20] Ibid.
[21] Ibid.
[22] Chris Johnson, "Draft International Code of Conduct for Outer Space Activities Fact Sheet," Secure World Foundation, Updated February 2014, https://swfound.org/media/166384/swf_draft_international_code_of_conduct_for_outer_space_activities_fact_sheet_february_2014.pdf.
[23] Jeff Abramson, "EU Issues Space Code of Conduct," *Arms Control Today*, January 16, 2009, https://armscontrol.org/act/2009_01-02/eu_issues_space_code_conduct.
[24] Chris Johnson, "Draft International Code of Conduct for Outer Space Activities Fact Sheet."
[25] Hitchens, "Forwarding Multilateral Space Governance: Next Steps for the International Community." Michael J. Listner, "The International Code of Conduct: Comments on changes in the latest draft and post-mortem thoughts," *The Space Review*, October 26, 2015, http://www.thespacereview.com/article/2851/1. Rajeswari Pillai Rajagopalan and Daniel A. Porras, "Commentary | EU Courts Support for Space Code of Conduct," *SpaceNews*, July 14, 2014, https://spacenews.com/41254eu-courts-support-for-space-code-of-conduct/.
[26] Paul B. Larsen, "Space Traffic Management Standards," *Journal of Air Law and Commerce* 83, no. 2 (2018): 379, https://scholar.smu.edu/cgi/viewcontent.cgi?article=4087&context=jalc.
[27] CONFERS, accessed February 28, 2019, https://www.satelliteconfers.org.
[28] Debra Werner, "DARPA working group begins addressing concerns related to proximity operations and satellite servicing," *SpaceNews*, May 23, 2018, https://spacenews.com/darpa-group-addresses-security-concerns/.
[29] Ian Christensen, "Forum 360: On-Orbit Servicing: Status and Progress of a Revolutionary Capability," AIAA Space 2018 Conference, September 16, 2018, Video, 47:50-54:00, https://livestream.com/AIAAvideo/space2018/videos/180445220.
[30] Jacqueline Klimas and Bryan Bender, POLITICO Space, October 12, 2018, https://www.politico.com/newsletters/politico-space/2018/10/12/us-russian-solidarity-after-launch-safely-aborted-325432. Consortium for Execution of Rendezvous and Servicing Operations, "Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS)," November 7, 2018, https://www.politico.com/f/?id=00000166-f419-d3ac-a1fe-f7bfe45e0001.
[31] Bryan Bender, "Industry agrees on rules for in-orbit repairs," POLITICO Space, February 6, 2019, https://www.politico.com/newsletters/politico-space/2019/02/06/industry-agrees-on-rules-for-in-orbit-repairs-387568. Consortium for Execution of Rendezvous and Servicing Operations, "CONFERS Recommended Design and Operational Practices," February 1, 2019, https://www.satelliteconfers.org/wp-content/uploads/2019/02/CONFERS-Operating-Practices-Approved-1-Feb-2019-003.pdf.
[32] Christensen, "Forum 360: On-Orbit Servicing," Video, 47:50-54:00.

[33] DARPA, "Consortium for Execution of Rendezvous and Servicing Operations (CONFERS)," accessed February 28, 2019, https://www.darpa.mil/program/consortium-for-execution-of-rendezvous-and-servicing-operations.
[34] McGill, "Manual on International Law Applicable to Military Uses of Outer Space," accessed April 13, 2019, https://www.mcgill.ca/milamos/.
[35] Ibid.
[36] McGill, "Manual on International Law Applicable to Military Uses of Outer Space: Our People," accessed April 13, 2019, https://www.mcgill.ca/milamos/our-people.
[37] McGill, "Manual on International Law Applicable to Military Uses of Outer Space: About MILAMOS," accessed April 13, 2019, https://www.mcgill.ca/milamos/about.
[38] Ibid.
[39] The University of Adelaide, "The Woomera Manual," accessed March 3, 2019, https://law.adelaide.edu.au/woomera/home.
[40] Ibid.
[41] The University of Adelaide, "The Woomera Manual on the International Law of Military Space Operations," Information Booklet, October 2018, https://law.adelaide.edu.au/woomera/system/files/docs/Woomera%20Manual.pdf.
[42] Jacqueline Klimas, "2 Japanese space companies growing U.S. operations," POLITICO Space, February 4, 2019, https://www.politico.com/newsletters/politico-space/2019/02/04/2-japanese-space-companies-growing-us-operations-385281.
[43] Geneva Internet Platform Digital Watch, "UN GGE," accessed February 28, 2019, https://dig.watch/processes/ungge.
[44] Elaine Korzak, "UN GGE on Cybersecurity: The End of an Era?" *The Diplomat*, July 31, 2017, https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.
[45] Ibid.
[46] James Shires, "Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States," *War on the Rocks*, October 12, 2018, https://warontherocks.com/2018/10/between-multistakeholderism-and-sovereignty-cyber-norms-in-egypt-and-the-gulf-states/.
[47] Ibid.
[48] Organization for Security and Co-operation in Europe, "Permanent Council Decision No. 1106," December 3, 2013, https://www.osce.org/pc/109168. Organization for Security and Co-operation in Europe, "Permanent Council Decision No. 1202," March 10, 2016, http://www.osce.org/pc/227281.
[49] Organization for Security and Co-operation in Europe, CSCE/OSCE key documents, accessed February 28, 2019, https://www.osce.org/resources/csce-osce-key-documents.
[50] Theresa Hitchens and Nancy W. Gallagher, "Building Confidence in the Cybersphere: A Path to Multilateral Progress," CISSM Working Paper, March 2018, https://www.cissm.umd.edu/publications/building-confidence-cybersphere-path-multilateral-progress.
[51] Ibid.
[52] Ibid.
[53] European Commission, "The Directive on security of network and information systems (NIS Directive)," August 24, 2018, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
[54] EUR-Lex, Document 32016L1148, accessed February 28, 2019, https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.
[55] Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," Citizen Lab, September 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/.
[56] Shanghai Cooperation Organisation, "About SCO," January 9, 2017, http://eng.sectsco.org/about_sco/.
[57] Eleanor Albert, "The Shanghai Cooperation Organization," Council on Foreign Relations, October 14, 2015, https://www.cfr.org/backgrounder/shanghai-cooperation-organization.
[58] McKune, "An Analysis of the International Code of Conduct for Information Security."
[59] Ibid.
[60] Ibid.
[61] Ibid.

[62] Alex Grigsby, "Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?" Council on Foreign Relations, January 28, 2015, https://www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era.
[63] Ibid.
[64] Ibid.
[65] International Telecommunications Union, "World Conference on International Telecommunications (WCIT-12)," accessed February 28, 2019, https://www.itu.int/en/wcit-12/Pages/default.aspx.
[66] International Telecommunications Union, "Final Acts: World Conference on International Telecommunications," 2012, https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.
[67] Cyrus Farivar, "The UN's telecom conference is finally over. Who won? Nobody knows." *Ars Technica*, December 14, 2012, https://arstechnica.com/tech-policy/2012/12/the-uns-telecom-conference-is-finally-over-who-won-nobody-knows/.
[68] Danielle Kehl and Tim Maurer, "Did the U.N. Internet Governance Summit Actually Accomplish Anything?" *Slate*, December 14, 2012, https://slate.com/technology/2012/12/wcit-2012-has-ended-did-the-u-n-internet-governance-summit-accomplish-anything.html.
[69] Ibid.
[70] Global Commission on the Stability of Cyberspace, "Home," accessed April 16, 2019, https://cyberstability.org.
[71] Geneva Internet Platform Digital Watch, "Global Commission on the Stability of Cyberspace," accessed April 16, 2019, https://dig.watch/actors/global-commission-stability-cyberspace.
[72] Global Commission on the Stability of Cyberspace, "Home."
[73] Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," Council on Foreign Relations, November 15, 2018, https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.
[74] Ibid.
[75] Ibid.
[76] Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law*, 2017, https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.
[77] Michael N. Schmitt, ed., "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations," Second Edition, Cambridge University Press (2017): 1-3.
[78] Ibid.
[79] White House, "National Space Policy of the United States," June 28, 2010, https://obamawhitehouse.archives.gov/sites/default/files/national_space_policy_6-28-10.pdf.
[80] Catherine Cheney, "W.H. releases National Space Policy," *POLITICO*, June 29, 2010, https://www.politico.com/story/2010/06/wh-releases-national-space-policy-039138.
[81] Ibid.
[82] William J. Broad and Kenneth Chang, "Obama Reverses Bush's Space Policy," *New York Times*, June 28, 2010, https://www.nytimes.com/2010/06/29/science/space/29orbit.html.
[83] White House, "National Space Policy of the United States," 7.
[84] Ibid, 4.
[85] Ibid, 10.
[86] Ibid, 7-8.
[87] Department of Defense and Office of the Director of National Intelligence, "National Security Space Strategy: Unclassified Summary," January 2011, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2011_nationalsecurityspacestrategy.pdf.
[88] Theresa Hitchens and Joan Johnson-Freese, "Toward a New National Security Space Strategy: Time for a Strategic Rebalancing," Atlantic Council Strategy Paper No. 5 (June 2016): 6, https://www.atlanticcouncil.org/images/publications/AC_StrategyPapers_No5_Space_WEB1.pdf.
[89] Laura Grego, "More on the National Security Space Strategy," All Things Nuclear (blog), Union of Concerned Scientists, February 10, 2011, http://allthingsnuclear.org/lgrego/more-on-the-national-security-space-strategy.

[90] Department of Defense and Office of the Director of National Intelligence, "National Security Space Strategy: Unclassified Summary," 5-6.
[91] Ibid, 4, 7.
[92] Ibid, 14.
[93] Ibid, i.
[94] White House, "National Space Transportation Policy," November 21, 2013, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_space_transportation_policy_11212013.pdf.
[95] Jeff Foust, "New national space transportation policy makes modest, not major, changes," Space Politics, November 22, 2013, http://www.spacepolitics.com/2013/11/22/new-national-space-transportation-policy-makes-modest-not-major-changes/.
[96] White House, "National Space Transportation Policy," 7.
[97] White House, "National Space Weather Strategy," Product of the National Science and Technology Council, October 2015, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/final_nationalspaceweatherstrategy_20151028.pdf.
[98] National Oceanic and Atmospheric Administration, "NOAA Commercial Space Policy," January 2016, https://www.corporateservices.noaa.gov/ames/administrative_orders/chapter_217/Commercial%20Space%20Policy.pdf.
[99] Ibid, 3.
[100] Ibid, 4.
[101] White House, "Presidential Executive Order on Reviving the National Space Council," June 30, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-reviving-national-space-council/.
[102] Ibid.
[103] SpaceNews Staff, "BREAKING | President Trump reestablishes National Space Council," *SpaceNews*, June 30, 2017, https://spacenews.com/breaking-president-trump-reestablishes-national-space-council/.
[104] Jeff Foust, "New National Space Strategy emphasizes 'America first' policies," *SpaceNews*, March 24, 2018, https://spacenews.com/new-national-space-strategy-emphasizes-america-first-policies/.
[105] White House, "President Donald J. Trump is Unveiling an America First National Space Strategy: Fact Sheet," March 23, 2018, https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/.
[106] Ibid.
[107] White House, "Presidential Memorandum on Reinvigorating America's Human Space Exploration Program," December 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-reinvigorating-americas-human-space-exploration-program/.
[108] White House, "Space Policy Directive-2, Streamlining Regulations on Commercial Use of Space," May 24, 2018, https://www.whitehouse.gov/presidential-actions/space-policy-directive-2-streamlining-regulations-commercial-use-space/.
[109] Todd Harrison and Kaitlyn Johnson, "How Might Space Policy Directive 2 Affect Commercial Space?" CSIS, May 30, 2018, https://www.csis.org/analysis/how-might-space-policy-directive-2-affect-commercial-space.
[110] White House, "Space Policy Directive-3, National Space Traffic Management Policy," June 18, 2018, https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/.
[111] Todd Harrison and Kaitlyn Johnson, "How Does Space Policy Directive 3 Affect Space Traffic Management?" CSIS, June 19, 2018, https://www.csis.org/analysis/how-does-space-policy-directive-3-affect-space-traffic-management.
[112] White House, "Text of Space Policy Directive-4: Establishment of the United States Space Force," February 19, 2019, https://www.whitehouse.gov/presidential-actions/text-space-policy-directive-4-establishment-united-states-space-force/.
[113] Ibid.
[114] Ibid.

[115] Kaitlyn Johnson, "How Does Space Policy Directive-4 Reorganize U.S. Military Space Operations?" CSIS, February 20, 2019, https://www.csis.org/analysis/how-does-space-policy-directive-4-reorganize-us-military-space-operations.
[116] White House, "Cyberspace Policy Review," 2009, https://fas.org/irp/eprint/cyber-review.pdf, iii.
[117] Ibid, iii.
[118] Ibid, 5.
[119] Ibid, 15, 17, 31.
[120] White House, "International Strategy for Cyberspace," May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[121] Howard A. Schmidt, "Launching the U.S. International Strategy for Cyberspace," White House, May 16, 2011, https://obamawhitehouse.archives.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace.
[122] Ibid.
[123] White House, "International Strategy for Cyberspace," 12.
[124] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.
[125] "Defense Department Strategy for Operating in Cyberspace," Defense Department via Breaking Gov, no date, https://breakinggov.com/documents/defense-department-cyber-strategy-report/.
[126] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 11.
[127] White House, "Executive Order -- Improving Critical Infrastructure Cybersecurity," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[128] Eric A. Fischer, "Infrastructure Protection, and Security Technologies Committee on Homeland Security," U.S. House of Representatives, Hearing on "Oversight of Executive Order 13636 and Development of the Cybersecurity Framework," July 18, 2013, https://docs.house.gov/meetings/HM/HM08/20130718/101151/HHRG-113-HM08-Wstate-FisherE-20130718.pdf.
[129] Department of Homeland Security, "Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD-21 Critical Infrastructure Security and Resilience," March 2013, https://www.dhs.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf.
[130] White House, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[131] Ibid.
[132] Ibid.
[133] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
[134] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, 1.
[135] Ibid.
[136] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, April 16, 2018, ii, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[137] Department of Defense, "The Department of Defense Cyber Strategy," April 2015, http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.
[138] Ibid, Letter Signed by Ash Carter.
[139] Ibid, 11.
[140] Ibid, 18.
[141] Ibid, 27.
[142] Denise E. Zheng, "2015 DOD Cyber Strategy," CSIS, April 24, 2015, https://www.csis.org/analysis/2015-dod-cyber-strategy.
[143] Ibid.
[144] Ibid.

[145] White House, "FACT SHEET: Cybersecurity National Action Plan," February 9, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.
[146] Ibid.
[147] Ibid.
[148] Department of State, "Department of State International Cyberspace Policy Strategy," March 2016, https://www.state.gov/documents/organization/255732.pdf.
[149] White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.
[150] Thomas P. Barletta et al., "Executive Order Addresses Federal Network and Infrastructure Cybersecurity Issues," Steptoe, May 31, 2017, https://www.steptoe.com/en/news-publications/executive-order-addresses-federal-network-and-infrastructure-cybersecurity-issues.html.
[151] Department of Defense, "Summary: Department of Defense Cyber Strategy," 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[152] Department of Defense, "Fact Sheet: 2018 DoD Cyber Strategy and Cyber Posture Review," September 18, 2018, https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pdf.
[153] Ibid.
[154] White House, "National Cyber Strategy of the United States of America," September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[155] Grant Schneider, "President Trump Unveils America's First Cybersecurity Strategy in 15 Years," White House, September 20, 2018, https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.
[156] White House, "National Cyber Strategy of the United States of America," 10.
[157] Ibid, 8, 16.
[158] Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased."
[159] Alex Grigsby, "The Year in Review: The Death of the UN GGE Process?" Council on Foreign Relations, December 21, 2017, https://www.cfr.org/blog/year-review-death-un-gge-process.
[160] Shires, "Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States."
[161] Hitchens and Gallagher, "Building Confidence in the Cybersphere: A Path to Multilateral Progress," 4-5.
[162] Shaun Waterman, "Experts push back on Trump administration's call to respond to cyberattacks with nukes," *Cyberscoop*, February 3, 2018, https://www.cyberscoop.com/nuclear-posture-review-cyberattacks-nukes-donald-trump/.
[163] Karen Singer, "100th space sharing agreement signed, Romania Space Agency joins," U.S. Strategic Command Public Affairs, April 29, 2019, https://www.af.mil/News/Article-Display/Article/1828045/100th-space-sharing-agreement-signed-romania-space-agency-joins/.
[164] Brian Weeden and Victoria Samson, "Op-ed | India's ASAT test is wake-up call for norms of behavior in space," *SpaceNews*, April 8, 2019, https://spacenews.com/op-ed-indias-asat-test-is-wake-up-call-for-norms-of-behavior-in-space/.
[165] Sandra Erwin, "Space Information Sharing and Analysis Center to be based in Colorado Springs," *SpaceNews*, April 8, 2019, https://spacenews.com/space-information-sharing-and-analysis-center-to-be-based-in-colorado-springs/.
[166] Ibid.
[167] Hitchens and Gallagher, "Building Confidence in the Cybersphere: A Path to Multilateral Progress," 7.
[168] James Andrew Lewis, "Sustaining Progress in International Negotiations on Cybersecurity," CSIS, July 25, 2017, https://www.csis.org/analysis/sustaining-progress-international-negotiations-cybersecurity.
[169] Hitchens and Gallagher, "Building Confidence in the Cybersphere: A Path to Multilateral Progress," 7.
[170] Shires, "Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States."
[171] Cory Bennett, "Why Trump is sticking with Obama's China hacking deal," *POLITICO*, November 8, 2017, https://www.politico.com/story/2017/11/08/trump-obama-china-hacking-deal-244658.
[172] Ibid.

[173] Christopher Bing, "U.S. accuses China of violating bilateral anti-hacking deal," Reuters, November 8, 2018, https://www.reuters.com/article/us-usa-china-cyber/u-s-accuses-china-of-violating-bilateral-anti-hacking-deal-idUSKCN1NE02E.

Bibliography

Abramson, Jeff. “EU Issues Space Code of Conduct.” *Arms Control Today*, January 16, 2009. https://armscontrol.org/act/2009_01-02/eu_issues_space_code_conduct.

Albert, Eleanor. “The Shanghai Cooperation Organization.” Council on Foreign Relations, October 14, 2015. https://www.cfr.org/backgrounder/shanghai-cooperation-organization.

Barletta, Thomas P., Paul R. Hurst, and Kendall R. Enyard. “Executive Order Addresses Federal Network and Infrastructure Cybersecurity Issues.” Steptoe, May 31, 2017. https://www.steptoe.com/en/news-publications/executive-order-addresses-federal-network-and-infrastructure-cybersecurity-issues.html.

Bender, Bryan. “Industry agrees on rules for in-orbit repairs.” POLITICO Space, February 6, 2019. https://www.politico.com/newsletters/politico-space/2019/02/06/industry-agrees-on-rules-for-in-orbit-repairs-387568.

Bennett, Cory. “Why Trump is sticking with Obama's China hacking deal.” *POLITICO*, November 8, 2017. https://www.politico.com/story/2017/11/08/trump-obama-china-hacking-deal-244658.

Bing, Christopher. “U.S. accuses China of violating bilateral anti-hacking deal.” Reuters, November 8, 2018. https://www.reuters.com/article/us-usa-china-cyber/u-s-accuses-china-of-violating-bilateral-anti-hacking-deal-idUSKCN1NE02E.

Broad, William J. and Kenneth Chang. “Obama Reverses Bush’s Space Policy.” *New York Times*, June 28, 2010. https://www.nytimes.com/2010/06/29/science/space/29orbit.html.

Cheney, Catherine. “W.H. releases National Space Policy.” *POLITICO*, June 29, 2010. https://www.politico.com/story/2010/06/wh-releases-national-space-policy-039138.

Christensen, Ian. “Forum 360: On-Orbit Servicing: Status and Progress of a Revolutionary Capability.” AIAA Space 2018 Conference, September 16, 2018. Video, 47:50-54:00. https://livestream.com/AIAAvideo/space2018/videos/180445220.

CONFERS. Accessed February 28, 2019. https://www.satelliteconfers.org.

Consortium for Execution of Rendezvous and Servicing Operations. “CONFERS Recommended Design and Operational Practices.” February 1, 2019. https://www.satelliteconfers.org/wp-content/uploads/2019/02/CONFERS-Operating-Practices-Approved-1-Feb-2019-003.pdf.

Consortium for Execution of Rendezvous and Servicing Operations. “Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS).” November 7, 2018. https://www.politico.com/f/?id=00000166-f419-d3ac-a1fe-f7bfe45e0001.

DARPA. “Consortium for Execution of Rendezvous and Servicing Operations (CONFERS).” Accessed February 28, 2019. https://www.darpa.mil/program/consortium-for-execution-of-rendezvous-and-servicing-operations.

Department of Defense. “Department of Defense Strategy for Operating in Cyberspace.” July 2011. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.

Defense Department via Breaking Gov. “Defense Department Strategy for Operating in Cyberspace.” No date. https://breakinggov.com/documents/defense-department-cyber-strategy-report/.

Department of Defense. “Fact Sheet: 2018 DoD Cyber Strategy and Cyber Posture Review.” September 18, 2018. https://media.defense.gov/2018/Sep/18/2002041659/-1/-1/1/Factsheet_for_Strategy_and_CPR_FINAL.pdf.

Department of Defense. “Summary: Department of Defense Cyber Strategy.” 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Department of Defense. “The Department of Defense Cyber Strategy.” April 2015. http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.

Department of Defense and Office of the Director of National Intelligence. “National Security Space Strategy: Unclassified Summary.” January 2011. https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2011_nationalsecurityspacestrategy.pdf.

Department of Homeland Security. “Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD-21 Critical Infrastructure Security and Resilience.” March 2013. https://www.dhs.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf.

Department of State. “Department of State International Cyberspace Policy Strategy.” March 2016. https://www.state.gov/documents/organization/255732.pdf.

Erwin, Sandra. “Space Information Sharing and Analysis Center to be based in Colorado Springs.” *SpaceNews*, April 8, 2019. https://spacenews.com/space-information-sharing-and-analysis-center-to-be-based-in-colorado-springs/.

EUR-Lex. Document 32016L1148. Accessed February 28, 2019. https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

European Commission. “The Directive on security of network and information systems (NIS Directive).” August 24, 2018. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

European Union. “DRAFT International Code of Conduct for Outer Space Activities.” March 31, 2014. https://cdn3-eeas.fpfis.tech.ec.europa.eu/cdn/farfuture/05ntjiVf8oPvMqMbHUgmbT3jt81mZ8mAZUXdPiGiFwQ/mtime:1479119506/sites/eeas/files/space_code_conduct_draft_vers_31-march-2014_en.pdf.

Farivar, Cyrus. “The UN’s telecom conference is finally over. Who won? Nobody knows.” *Ars Technica*, December 14, 2012. https://arstechnica.com/tech-policy/2012/12/the-uns-telecom-conference-is-finally-over-who-won-nobody-knows/.

Fischer, Eric A. “Infrastructure Protection, and Security Technologies Committee on Homeland Security.” U.S. House of Representatives, Hearing on “Oversight of Executive Order 13636 and Development of the Cybersecurity Framework,” July 18, 2013. https://docs.house.gov/meetings/HM/HM08/20130718/101151/HHRG-113-HM08-Wstate-FisherE-20130718.pdf.

Foust, Jeff. “New National Space Strategy emphasizes ‘America first’ policies.” *SpaceNews*, March 24, 2018. https://spacenews.com/new-national-space-strategy-emphasizes-america-first-policies/.

Foust, Jeff. “New national space transportation policy makes modest, not major, changes.” Space Politics, November 22, 2013. http://www.spacepolitics.com/2013/11/22/new-national-space-transportation-policy-makes-modest-not-major-changes/.

Geneva Internet Platform Digital Watch. “Global Commission on the Stability of Cyberspace.” Accessed April 16, 2019. https://dig.watch/actors/global-commission-stability-cyberspace.

Geneva Internet Platform Digital Watch. “UN GGE.” Accessed February 28, 2019. https://dig.watch/processes/ungge.

Global Commission on the Stability of Cyberspace. “Home.” Accessed April 16, 2019. https://cyberstability.org.

Grego, Laura. “More on the National Security Space Strategy.” All Things Nuclear (blog). Union of Concerned Scientists. February 10, 2011. http://allthingsnuclear.org/lgrego/more-on-the-national-security-space-strategy.

Grigsby, Alex. “The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased.” Council on Foreign Relations, November 15, 2018. https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

Grigsby, Alex. “The Year in Review: The Death of the UN GGE Process?” Council on Foreign Relations, December 21, 2017. https://www.cfr.org/blog/year-review-death-un-gge-process.

Grigsby, Alex. “Will China and Russia’s Updated Code of Conduct Get More Traction in a Post-Snowden Era?” Council on Foreign Relations, January 28, 2015. https://www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era.

Harrison, Todd and Kaitlyn Johnson. “How Does Space Policy Directive 3 Affect Space Traffic Management?” CSIS, June 19, 2018. https://www.csis.org/analysis/how-does-space-policy-directive-3-affect-space-traffic-management.

Harrison, Todd and Kaitlyn Johnson. “How Might Space Policy Directive 2 Affect Commercial Space?” CSIS, May 30, 2018. https://www.csis.org/analysis/how-might-space-policy-directive-2-affect-commercial-space.

Hitchens, Theresa and Nancy W. Gallagher. “Building Confidence in the Cybersphere: A Path to Multilateral Progress.” CISSM Working Paper, March 2018. https://www.cissm.umd.edu/publications/building-confidence-cybersphere-path-multilateral-progress.

Hitchens, Theresa. “Forwarding Multilateral Space Governance: Next Steps for the International Community.” CISSM Working Paper, August 2018. http://cissm.umd.edu/sites/default/files/ForwardingMultilateralSpaceGovernance%20updated82018.pdf.

Hitchens, Theresa and Joan Johnson-Freese. “Toward a New National Security Space Strategy: Time for a Strategic Rebalancing.” Atlantic Council Strategy Paper No. 5 (June 2016): 6, https://www.atlanticcouncil.org/images/publications/AC_StrategyPapers_No5_Space_WEB1.pdf.

International Telecommunications Union. “Final Acts: World Conference on International Telecommunications.” 2012. https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf.

International Telecommunications Union. “World Conference on International Telecommunications (WCIT-12).” Accessed February 28, 2019. https://www.itu.int/en/wcit-12/Pages/default.aspx.

Jakhu, R.S. and J.N. Pelton, eds. “Overview of the Existing Mechanisms of Global Space Governance.” Chapter 2 in *Global Space Governance: An International Study*. Springer International Publishing (2017): 32.

Jensen, Eric Talbot. “The Tallinn Manual 2.0: Highlights and Insights.” *Georgetown Journal of International Law*. 2017. https://www.law.georgetown.edu/international-law-journal/wp-content/uploads/sites/21/2018/05/48-3-The-Tallinn-Manual-2.0.pdf.

Johnson, Chris. “Draft International Code of Conduct for Outer Space Activities Fact Sheet.” Secure World Foundation, Updated February 2014. https://swfound.org/media/166384/swf_draft_international_code_of_conduct_for_outer_space_activities_fact_sheet_february_2014.pdf.

Johnson, Christopher. “The UN Group of Governmental Experts on Space TCBMs.” Secure World Foundation, Updated April 2014. https://swfound.org/media/109311/swf_gge_on_space_tcbms_fact_sheet_april_2014.pdf.

Johnson, Christopher D. and Victoria Samson. “A summer update on the COPUOS long-term sustainability guidelines.” *The Space Review*, July 24, 2017. http://www.thespacereview.com/article/3291/1.

Johnson, Kaitlyn. “How Does Space Policy Directive-4 Reorganize U.S. Military Space Operations?” CSIS, February 20, 2019. https://www.csis.org/analysis/how-does-space-policy-directive-4-reorganize-us-military-space-operations.

Kehl, Danielle and Tim Maurer. “Did the U.N. Internet Governance Summit Actually Accomplish Anything?” *Slate*, December 14, 2012. https://slate.com/technology/2012/12/wcit-2012-has-ended-did-the-u-n-internet-governance-summit-accomplish-anything.html.

Klimas, Jacqueline. “2 Japanese space companies growing U.S. operations.” POLITICO Space, February 4, 2019. https://www.politico.com/newsletters/politico-space/2019/02/04/2-japanese-space-companies-growing-us-operations-385281.

Klimas, Jacqueline and Bryan Bender. POLITICO Space, October 12, 2018. https://www.politico.com/newsletters/politico-space/2018/10/12/us-russian-solidarity-after-launch-safely-aborted-325432.

Korzak, Elaine. "UN GGE on Cybersecurity: The End of an Era?" *The Diplomat*, July 31, 2017. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

Larsen, Paul B. "Space Traffic Management Standards." *Journal of Air Law and Commerce* 83, no. 2 (2018): 379. https://scholar.smu.edu/cgi/viewcontent.cgi?article=4087&context=jalc.

Lewis, James Andrew. "Sustaining Progress in International Negotiations on Cybersecurity." CSIS, July 25, 2017. https://www.csis.org/analysis/sustaining-progress-international-negotiations-cybersecurity.

Listner, Michael J. "The International Code of Conduct: Comments on changes in the latest draft and post-mortem thoughts." *The Space Review*, October 26, 2015. http://www.thespacereview.com/article/2851/1.

McGill. "Manual on International Law Applicable to Military Uses of Outer Space." Accessed April 13, 2019. https://www.mcgill.ca/milamos/.

McGill. "Manual on International Law Applicable to Military Uses of Outer Space: About MILAMOS." Accessed April 13, 2019. https://www.mcgill.ca/milamos/about.

McGill. "Manual on International Law Applicable to Military Uses of Outer Space: Our People." Accessed April 13, 2019. https://www.mcgill.ca/milamos/our-people.

McKune, Sarah. "An Analysis of the International Code of Conduct for Information Security." Citizen Lab, September 28, 2015. https://citizenlab.ca/2015/09/international-code-of-conduct/.

National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." Version 1.0. February 12, 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." Version 1.1. April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

National Oceanic and Atmospheric Administration. “NOAA Commercial Space Policy.” January 2016. https://www.corporateservices.noaa.gov/ames/administrative_orders/chapter_217/Commercial%20Space%20Policy.pdf.

Organization for Security and Co-operation in Europe. CSCE/OSCE key documents. Accessed February 28, 2019. https://www.osce.org/resources/csce-osce-key-documents.

Organization for Security and Co-operation in Europe. “Permanent Council Decision No. 1106.” December 3, 2013. https://www.osce.org/pc/109168.

Organization for Security and Co-operation in Europe. “Permanent Council Decision No. 1202.” March 10, 2016. http://www.osce.org/pc/227281.

Porras, Daniel. “Brief of UN Space Security Dialogues” in “Space Alert,” Volume VI, Issue 4. Observer Research Foundation, November 1, 2018. https://www.orfonline.org/research/space-alert-volume-vi-issue-4-45315/.

Rajagopalan, Rajeswari Pillai and Daniel A. Porras. “Commentary | EU Courts Support for Space Code of Conduct.” *SpaceNews*, July 14, 2014. https://spacenews.com/41254eu-courts-support-for-space-code-of-conduct/.

Schmidt, Howard A. “Launching the U.S. International Strategy for Cyberspace.” White House, May 16, 2011. https://obamawhitehouse.archives.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace.

Schmitt, Michael N., ed. “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.” Second Edition. Cambridge University Press (2017): 1-3.

Schneider, Grant. “President Trump Unveils America’s First Cybersecurity Strategy in 15 Years.” White House, September 20, 2018. https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.

Secure World Foundation. “SWF Highlights Implementation of Sustainability Guidelines and Commercial Satellite Servicing Standards at UN.” February 18, 2019. https://swfound.org/news/all-news/2019/02/swf-highlights-implementation-of-sustainability-guidelines-and-commercial-satellite-servicing-standards-at-un.

Shanghai Cooperation Organisation. “About SCO.” January 9, 2017. http://eng.sectsco.org/about_sco/.

Shires, James. “Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States.” *War on the Rocks*, October 12, 2018. https://warontherocks.com/2018/10/between-multistakeholderism-and-sovereignty-cyber-norms-in-egypt-and-the-gulf-states/.

Singer, Karen. “100th space sharing agreement signed, Romania Space Agency joins.” U.S. Strategic Command Public Affairs, April 29, 2019. https://www.af.mil/News/Article-Display/Article/1828045/100th-space-sharing-agreement-signed-romania-space-agency-joins/.

SpaceNews Staff. “BREAKING | President Trump reestablishes National Space Council.” *SpaceNews*, June 30, 2017. https://spacenews.com/breaking-president-trump-reestablishes-national-space-council/.

The University of Adelaide. “The Woomera Manual.” Accessed March 3, 2019. https://law.adelaide.edu.au/woomera/home.

The University of Adelaide. “The Woomera Manual on the International Law of Military Space Operations.” Information Booklet. October 2018. https://law.adelaide.edu.au/woomera/system/files/docs/Woomera%20Manual.pdf.

UN Disarmament Commission. “2018 United Nations Disarmament Commission.” Non-paper by the Secretariat (Working Group II). https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/03/WG2-secretariat-non-paper-outer-space-TCBMs-FINAL.pdf.

UN Disarmament Commission. “Recommendations to promote the practical implementation of transparency and confidence-building measures in outer space activities with the goal of preventing an arms race in outer space, in accordance with the recommendations set out in the report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities.” Working paper submitted by Nigeria (on behalf of the African Group), A/CN.10/2019/WP.1, April 25, 2019. https://undocs.org/A/CN.10/2019/WP.1.

United Nations Office for Outer Space Activities. “Committee on the Peaceful Uses of Outer Space.” Accessed February 28, 2019. http://www.unoosa.org/oosa/en/ourwork/copuos/index.html.

United Nations Office for Outer Space Activities. “Committee on the Peaceful Uses of Outer Space: Membership Evolution.” Accessed February 28, 2019. http://www.unoosa.org/oosa/en/ourwork/copuos/members/evolution.html.

United Nations Office for Outer Space Activities. “COPUOS History.” Accessed February 28, 2019. http://www.unoosa.org/oosa/en/ourwork/copuos/history.html.

Waterman, Shaun. “Experts push back on Trump administration's call to respond to cyberattacks with nukes.” *Cyberscoop*, February 3, 2018. https://www.cyberscoop.com/nuclear-posture-review-cyberattacks-nukes-donald-trump/.

Weeden, Brian. “Testimony before the U.S.-China Economic and Security Review Commission.” Hearing on “China in Space: A Strategic Competition?” April 25, 2019. https://swfound.org/media/206425/weeden_uscc_testimony_april2019.pdf.

Weeden, Brian and Victoria Samson. “Op-ed | India’s ASAT test is wake-up call for norms of behavior in space.” *SpaceNews*, April 8, 2019, https://spacenews.com/op-ed-indias-asat-test-is-wake-up-call-for-norms-of-behavior-in-space/.

Werner, Debra. “DARPA working group begins addressing concerns related to proximity operations and satellite servicing.” *SpaceNews*, May 23, 2018. https://spacenews.com/darpa-group-addresses-security-concerns/.

White House. “Cyberspace Policy Review.” 2009. https://fas.org/irp/eprint/cyber-review.pdf.

White House. “Executive Order -- Improving Critical Infrastructure Cybersecurity.” February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

White House. “FACT SHEET: Cybersecurity National Action Plan.” February 9, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

White House. “International Strategy for Cyberspace.” May 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

White House. “National Cyber Strategy of the United States of America.” September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

White House. “National Space Policy of the United States.” June 28, 2010. https://obamawhitehouse.archives.gov/sites/default/files/national_space_policy_6-28-10.pdf.

White House. “National Space Transportation Policy.” November 21, 2013. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_space_transportation_policy_11212013.pdf.

White House. “National Space Weather Strategy.” Product of the National Science and Technology Council. October 2015. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/final_nationalspaceweatherstrategy_20151028.pdf.

White House. “President Donald J. Trump is Unveiling an America First National Space Strategy: Fact Sheet.” March 23, 2018. https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/.

White House. “Presidential Executive Order on Reviving the National Space Council.” June 30, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-reviving-national-space-council/.

White House. “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.” May 11, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

White House. “Presidential Policy Directive -- Critical Infrastructure Security and Resilience.” February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

White House. “Presidential Memorandum on Reinvigorating America’s Human Space Exploration Program.” December 11, 2017. https://www.whitehouse.gov/presidential-actions/presidential-memorandum-reinvigorating-americas-human-space-exploration-program/.

White House. “Space Policy Directive-2, Streamlining Regulations on Commercial Use of Space.” May 24, 2018. https://www.whitehouse.gov/presidential-actions/space-policy-directive-2-streamlining-regulations-commercial-use-space/.

White House. “Space Policy Directive-3, National Space Traffic Management Policy.” June 18, 2018. https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/.

White House. “Text of Space Policy Directive-4: Establishment of the United States Space Force.” February 19, 2019. https://www.whitehouse.gov/presidential-actions/text-space-policy-directive-4-establishment-united-states-space-force/.

Wolny, Josh. “The UN COPUOS Guidelines on the Long-term Sustainability of Outer Space Activities.” Secure World Foundation, Updated August 2018. https://swfound.org/media/206227/swf_un_copuos_lts_guidelines_fact_sheet_august_2018.pdf.

Wood, Robert. “Explanation of Vote in the First Committee on Resolution L.54: Further Practical Measures for the Prevention of an Arms Race in Outer Space.” United States Mission to the United Nations, October 20, 2017. https://usun.state.gov/remarks/8085.

Zheng, Denise E. “2015 DOD Cyber Strategy.” CSIS, April 24, 2015. https://www.csis.org/analysis/2015-dod-cyber-strategy.

Appendix: Tables for Comparing Governance Initiatives

Multilateral Space Initiatives

Forum	Time Frame	Types of Participants	Goals or Purpose	Notable Outcomes	Soft vs Hard Law	Level of Success
Working Group on the Long-term Sustainability of Outer Space Activities, Committee on the Peaceful Uses of Outer Space (COPUOS), UN	2010-2018	Primary: member states; Secondary: observers (other stakeholders)	Develop guidelines on the long-term sustainability of outer space activities	Reached consensus on 12 guidelines in 2016 and 9 more guidelines in 2018	Soft law	Successful: members reached consensus on 21 LTS guidelines [10] (Note: Russia blocked approval of a final report on the guidelines [11])
GGE on Transparency and Confidence-Building Measures in Outer Space Activities, UN	2011-2013	Experts nominated by member states [3]	Make recommendations that "improve international cooperation and reduce the risks of misunderstanding, mistrust, and miscalculations in outer space activities" [4]	Issued report in 2013 [9]	Soft law	Successful: issued a final report (approved by consensus) [12]
GGE on Further Practical Measures for the Prevention of an Arms Race in Outer Space, UN	2018-2019	Experts nominated by member states	Make recommendations on "an international legally binding instrument on the prevention of an arms race in outer space" [5]	Failed to reach consensus on a final report	Soft law	Unsuccessful: failed to reach consensus on a final report [13, 14]
European Union - Code of Conduct	2007-2014 [1, 2]	Primary: member states; Secondary: non-EU states and other stakeholders	Develop a proposal for “outer space transparency and confidence-building measures,” as directed in a 2006 UNGA resolution [6]	Draft International Code of Conduct for Outer Space Activities first published in 2008; repeatedly revised; most recent draft from 2014	Soft law	Mixed success: although it had success in creating a draft internally, the Code did not gain international support and was not adopted for further discussion at the UN [15, 16, 17]
Consortium for Execution of Rendezvous and Servicing Operations (CONFERS)	2018-Present	Industry, academia, government, and experts	Develop best practices for OOS and RPO	Released its “Guiding Principles for Commercial Rendezvous and Proximity Operations (RPO) and On-Orbit Servicing (OOS)” in 2018	Best practices	In progress

The Woomera Manual on the International Law of Military Space Operations	2019-Present	Experts	"develop a Manual that objectively articulates and clarifies existing international law applicable to military space operations" [7]	In process	N/A	In progress
Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS)	2016-Present	Experts	"develop a widely-accepted manual clarifying the fundamental rules applicable to the military use of outer space in times of peace and in periods of rising tension" [8]	In process, scheduled to be completed in 3 years (so in 2019)	N/A	In progress

[1] Chris Johnson, "Draft International Code of Conduct for Outer Space Activities Fact Sheet," Secure World Foundation, Updated February 2014, https://swfound.org/media/166384/swf_draft_international_code_of_conduct_for_outer_space_activities_fact_sheet_february_2014.pdf.
[2] European Union, "DRAFT International Code of Conduct for Outer Space Activities," March 31, 2014, https://cdn3-eeas.fpfis.tech.ec.europa.eu/cdn/farfuture/05ntjiVf8oPvMqMbHUgmbT3jt81mZ8mAZUXdPiGiFwQ/mtime:1479119506/sites/eeas/files/space_code_conduct_draft_vers_31-march-2014_en.pdf.
[3] Christopher Johnson, "The UN Group of Governmental Experts on Space TCBMs," Updated April 2014, https://swfound.org/media/109311/swf_gge_on_space_tcbms_fact_sheet_april_2014.pdf.
[4] Ibid.
[5] UN Disarmament Commission, "2018 United Nations Disarmament Commission," Non-paper by the Secretariat (Working Group II), https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/03/WG2-secretariat-non-paper-outer-space-TCBMs-FINAL.pdf.
[6] Jeff Abramson, "EU Issues Space Code of Conduct," Arms Control Today, January 16, 2009, https://armscontrol.org/act/2009_01-02/eu_issues_space_code_conduct.
[7] The University of Adelaide, "The Woomera Manual," accessed March 3, 2019, https://law.adelaide.edu.au/woomera/home.
[8] McGill, "Manual on International Law Applicable to Military Uses of Outer Space," accessed April 13, 2019, https://www.mcgill.ca/milamos/.
[9] United Nations General Assembly, "Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities," A/68/189, July 29, 2013, http://undocs.org/A/68/189.
[10] Secure World Foundation, "SWF Highlights Implementation of Sustainability Guidelines and Commercial Satellite Servicing Standards at UN," February 18, 2019, https://swfound.org/news/all-news/2019/02/swf-highlights-implementation-of-sustainability-guidelines-and-commercial-satellite-servicing-standards-at-un.
[11] Theresa Hitchens, "Forwarding Multilateral Space Governance: Next Steps for the International Community," CISSM Working Paper, August 2018, http://cissm.umd.edu/sites/default/files/ForwardingMultilateralSpaceGovernance%20updated82018.pdf.
[12] Christopher Johnson, "The UN Group of Governmental Experts on Space TCBMs," Updated April 2014, https://swfound.org/media/109311/swf_gge_on_space_tcbms_fact_sheet_april_2014.pdf.
[13] Brian Weeden, "Testimony before the U.S.-China Economic and Security Review Commission," Hearing on "China in Space: A Strategic Competition?" April 25, 2019, 15, https://swfound.org/media/206425/weeden_uscc_testimony_april2019.pdf.
[14] UN Disarmament Commission, "Recommendations to promote the practical implementation of transparency and confidence-building measures in outer space activities with the goal of preventing an arms race in outer space, in accordance with the recommendations set out in the report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities," Working paper submitted by Nigeria (on behalf of the African Group), A/CN.10/2019/WP.1, April 25, 2019, https://undocs.org/A/CN.10/2019/WP.1. See paragraphs 7, 25, 26, and 51.
[15] Hitchens, "Forwarding Multilateral Space Governance: Next Steps for the International Community."
[16] Michael J. Listner, "The International Code of Conduct: Comments on changes in the latest draft and post-mortem thoughts," *The Space Review*, October 26, 2015, http://www.thespacereview.com/article/2851/1.
[17] Rajeswari Pillai Rajagopalan and Daniel A. Porras, "Commentary | EU Courts Support for Space Code of Conduct," *SpaceNews*, July 14, 2014, https://spacenews.com/41254eu-courts-support-for-space-code-of-conduct/.

Multilateral Cyber Initiatives

Forum	Time Frame	Types of Participants	Goals or Purpose	Notable Outcomes	Soft vs Hard Law	Level of Success
Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN	Six GGEs: 2004-5, 2009-10, 2012-13, 2014-15, 2016-17, 2019-21	Experts nominated by member states	Consider cooperative measures to strengthen information security at the global level and promote international cooperation in this field	Produced consensus reports in 2010, 2013, and 2015 (from the Second, Third, and Fourth GGEs); did not reach consensus in 2005 (First GGE) or in 2017 (Fifth GGE)	Soft law	Mixed success: (a) success in achieving consensus reports in 3 of 5 GGEs, although did not achieve consensus reports in 2 of 5 GGEs; (b) GGEs credited with "outlining the global cybersecurity agenda" and "introducing the principle that international law applies to the digital space" [8]
Informal Working Group, Organization for Security and Co-operation in Europe	2012-2016	Member states	"draft confidence-building measures (CBMs) to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs" [2]	Agreed upon 16 CBMs, 11 in 2013 and 5 in 2016	Soft law	Successful: agreed upon two sets of CMBs, 16 in total, which were adopted by the OSCE [9, 10, 11]
European Union	Standing Organization	Member states	Operate as political and economic union (regional organization)	Approved legislation	Hard law	Successful: EU adopted the Directive on Security of Network and Information Systems in 2016; states directed to transpose into national law (2018 deadline)
Shanghai Cooperation Organisation	Standing Organization	Member states	Explore consensus and cooperation on non-traditional security threats [3]	Created and revised International Code of Conduct for Information Security	Soft law	Mixed success: achieved consensus on Code within SCO; failed to make progress at the UN [12]
ITU World Conference on International Telecommunications	December 2012	Primary: states; Secondary: observers (other stakeholders)	Review the International Telecommunication Regulations (ITRs) (legally binding treaty) [4]	"Final Acts" document to update ITRs completed, although controversially [7]	Hard law (amended articles) and soft law (appendices) [7]	Mixed success: created new agreement, but major split- some states signed on to new agreement while others didn't [13, 14]

Open-Ended Working Group, UN	Standing Organization	States	"study the existing norms contained in the previous UN GGE reports, identify new norms, and study the possibility of 'establishing regular institutional dialogue …'" [5]	In progress	In progress	In progress
Tallinn Manuals/Cooperative Cyber Defense Center of Excellence, NATO	2009-2017	Experts	Create manual on international law governing cyber operations	Produced two manuals	N/A	Successful: produced two manuals
Global Commission on the Stability of Cyberspace	2017-Present	Experts	"develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace" [6]	Issued norm proposals	Soft law	Successful: issued two calls for protection and one norms package

[1] Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," Council on Foreign Relations, November 15, 2018, https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.
[2] Organization for Security and Co-operation in Europe, "Permanent Council Decision No. 1039," April 26, 2012, https://www.osce.org/pc/90169.
[3] Sarah McKune, "An Analysis of the International Code of Conduct for Information Security," Citizen Lab, September 28, 2015, https://citizenlab.ca/2015/09/international-code-of-conduct/.
[4] International Telecommunications Union, "World Conference on International Telecommunications (WCIT-12)," accessed February 28, 2019, https://www.itu.int/en/wcit-12/Pages/default.aspx.
[5] Alex Grigsby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," Council on Foreign Relations, November 15, 2018, https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.
[6] Global Commission on the Stability of Cyberspace, "Home," accessed April 16, 2019, https://cyberstability.org.
[7] Cyrus Farivar, "The UN's telecom conference is finally over. Who won? Nobody knows." *Ars Technica*, December 14, 2012, https://arstechnica.com/tech-policy/2012/12/the-uns-telecom-conference-is-finally-over-who-won-nobody-knows/.
[8] Geneva Internet Platform Digital Watch, "UN GGE," accessed February 28, 2019, https://dig.watch/processes/ungge.
[9] Organization for Security and Co-operation in Europe, "Permanent Council Decision No. 1106," December 3, 2013, https://www.osce.org/pc/109168.
[10] Organization for Security and Co-operation in Europe, "Permanent Council Decision No. 1202," March 10, 2016, http://www.osce.org/pc/227281.
[11] Organization for Security and Co-operation in Europe, "2018 OSCE-wide Conference on Cyber/ICT Security," September 27, 2018, https://www.osce.org/chairmanship/397514.
[12] McKune, "An Analysis of the International Code of Conduct for Information Security."
[13] Farivar, "The UN's telecom conference is finally over. Who won? Nobody knows."
[14] Danielle Kehl and Tim Maurer, "Did the U.N. Internet Governance Summit Actually Accomplish Anything?" *Slate*, December 14, 2012, https://slate.com/technology/2012/12/wcit-2012-has-ended-did-the-u-n-internet-governance-summit-accomplish-anything.html.

U.S. Space Policy

Policy	Policy Type	Release Date	Drivers or Motivations	Commercial Sector or Interests	Arms Control Issues	"Global Commons" Issues	Overlap Between Space and Cyber
National Space Policy	White House [1]	June 2010	Update guidance for government activities in space [12]	Yes	Yes	Yes	No
National Security Space Strategy: Unclassified Summary	DOD/ODNI [2]	January 2011	Provide greater focus on national security beyond 2010 NSP	Yes	Yes	Yes	No
National Space Transportation Policy	White House [3]	November 2013	Update and replace 2004 U.S. Space Transportation Policy [13]	Yes	No	No	No
National Space Weather Strategy	White House [4]	October 2015	Develop strategy "to enhance national preparedness for space-weather events"	No	No	No	No
NOAA Commercial Space Policy	NOAA [5]	January 2016	Part of push to procure weather data from the commercial sector	Yes	No	No	No
Executive Order Reviving the National Space Council	White House [6]	June 2017	"provide a coordinated process for developing and monitoring the implementation of national space policy and strategy"	Yes	No	No	No
Space Policy Directive-1	White House [7]	December 2017	Formalized space exploration goals	No	No	No	No
National Space Strategy	White House [8]	March 2018	Update Obama era space policy	Yes	No	No	No
Space Policy Directive-2	White House [9]	May 2018	Fix complex regulations unfriendly to commercial space sector	Yes	No	No	No
Space Policy Directive-3	White House [10]	June 2018	Rapidly increasing objects in space, need for improved STM and SSA	Yes	No	No	No
Space Policy Directive-4	White House [11]	February 2019	Formalized White House plan to establish Space Force	No	No	No	No

[1] White House, “National Space Policy of the United States,” June 28, 2010, https://obamawhitehouse.archives.gov/sites/default/files/national_space_policy_6-28-10.pdf.
[2] Department of Defense and Office of the Director of National Intelligence, “National Security Space Strategy: Unclassified Summary,” January 2011, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2011_nationalsecurityspacestrategy.pdf.
[3] White House, “National Space Transportation Policy,” November 21, 2013, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_space_transportation_policy_11212013.pdf.
[4] White House, “National Space Weather Strategy,” Product of the National Science and Technology Council, October 2015, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/final_nationalspaceweatherstrategy_20151028.pdf.
[5] National Oceanic and Atmospheric Administration, “NOAA Commercial Space Policy,” January 2016, https://www.corporateservices.noaa.gov/ames/administrative_orders/chapter_217/Commercial%20Space%20Policy.pdf.
[6] White House, “Presidential Executive Order on Reviving the National Space Council,” June 30, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-reviving-national-space-council/.
[7] White House, “Presidential Memorandum on Reinvigorating America’s Human Space Exploration Program,” December 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-reinvigorating-americas-human-space-exploration-program/.
[8] White House, “President Donald J. Trump is Unveiling an America First National Space Strategy: Fact Sheet,” March 23, 2018, https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/.
[9] White House, “Space Policy Directive-2, Streamlining Regulations on Commercial Use of Space,” May 24, 2018, https://www.whitehouse.gov/presidential-actions/space-policy-directive-2-streamlining-regulations-commercial-use-space/.
[10] White House, “Space Policy Directive-3, National Space Traffic Management Policy,” June 18, 2018, https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/.
[11] White House, “Text of Space Policy Directive-4: Establishment of the United States Space Force,” February 19, 2019, https://www.whitehouse.gov/presidential-actions/text-space-policy-directive-4-establishment-united-states-space-force/.
[12] Office of Space Commerce, “National Space Policy,” accessed March 6, 2019, https://www.space.commerce.gov/policy/national-space-policy/.
[13] White House, “Fact Sheet: 2013 National Space Transportation Policy,” November 21, 2013, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national_space_transportation_policy_fact_sheet_11212013.pdf.

U.S. Cyber Policy

Policy	Policy Type	Release Date	Drivers or Motivations	Commercial Sector or Interests	Arms Control Issues	"Global Commons" Issues	Overlap Between Space and Cyber
Cyberspace Policy Review	White House [1]	May 2009	Identify areas for the White House/US to take action on improving cybersecurity for the nation	Yes	No	No	No
International Strategy for Cyberspace	White House [2]	May 2011	Set "agenda for partnering with other nations and peoples to achieve that vision"	Yes	No	No	No
DOD Strategy for Operating in Cyberspace	DOD [3]	July 2011	Create unified strategy for cyberspace [14]	Yes	No	No	No
Executive Order -- Improving Critical Infrastructure Cybersecurity	White House [4]	February 2013	Direct government efforts to protect critical infrastructure from cyber threats [15]	Yes	No	No	No
Presidential Policy Directive -- Critical Infrastructure Security and Resilience (PPD-21)	White House [5]	February 2013	Set "national policy on critical infrastructure security and resilience"	Yes	No	No	No
NIST Cybersecurity Framework Version 1.0	NIST [6]	February 2014	Directed by February 2013 executive order	Yes	No	No	No
DOD Cyber Strategy	DOD [7]	April 2015	Update to 2011 strategy "to be more transparent about U.S. military doctrine, policy, roles, and missions in cyberspace" [16]	Yes	No	No	No
Cybersecurity National Action Plan: Fact Sheet	White House [8]	February 2016	"capstone" of more than 7 years of work to direct federal government to improve cybersecurity for all	Yes	No	No	No
Department of State International Cyberspace Policy Strategy	State [9]	March 2016	Update submitted to Congress	No	No	No	No
Executive Order -- Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure	White House [10]	May 2017	Push executive branch agencies to address cybersecurity concerns	Yes	No	No	No
NIST Cybersecurity Framework Version 1.1	NIST [11]	April 18	"refines, clarifies, and enhances Version 1.0"	Yes	No	No	No
DOD Cyber Strategy	DOD [12]	September 2018	Replace 2015 strategy; explain how DOD "will implement the priorities of the National Defense Strategy in and through cyberspace"	Yes	No	No	No

National Cyber Strategy	White House [13]	September 2018	Replace previous cyber strategy from 2003; provide updated priorities for government agencies	Yes	No	No	Yes

[1] White House, “Cyberspace Policy Review,” 2009, https://fas.org/irp/eprint/cyber-review.pdf.
[2] White House, “International Strategy for Cyberspace,” May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[3] Department of Defense, “Department of Defense Strategy for Operating in Cyberspace,” July 2011, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf.
[4] White House, “Executive Order -- Improving Critical Infrastructure Cybersecurity,” February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[5] White House, “Presidential Policy Directive -- Critical Infrastructure Security and Resilience,” February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.
[6] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.0, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
[7] Department of Defense, “The Department of Defense Cyber Strategy,” April 2015, http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf.
[8] White House, “FACT SHEET: Cybersecurity National Action Plan,” February 9, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.
[9] Department of State, “Department of State International Cyberspace Policy Strategy,” March 2016, https://www.state.gov/documents/organization/255732.pdf.
[10] White House, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” May 11, 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.
[11] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[12] Department of Defense, “Summary: Department of Defense Cyber Strategy,” 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
[13] White House, “National Cyber Strategy of the United States of America,” September 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[14] “Defense Department Strategy for Operating in Cyberspace,” Defense Department via Breaking Gov, no date, https://breakinggov.com/documents/defense-department-cyber-strategy-report/.
[15] Department of Homeland Security, “Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD-21 Critical Infrastructure Security and Resilience,” March 2013, https://www.dhs.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf.
[16] Denise E. Zheng, “2015 DOD Cyber Strategy,” Center for Strategic and International Studies, April 24, 2015, https://www.csis.org/analysis/2015-dod-cyber-strategy.