Cyberstability Paper Series

New Conditions and Constellations in Cyber

The Pro and Contra of an Incidents at Sea Agreement for Cyberspace

Contra

Benjamin Bahney
Senior Fellow, Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR)
Jonathan Reiber
Senior Director for Cybersecurity Strategy and Policy, AttackIQ
Brandon Williams
Cybersecurity postdoctoral Fellow, Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR)

Pro

Alexander Klimburg, PhD
Director, Global Commission on the Stability of Cyberspace Initiative and Secretariat

December 2021

Cyberstability Paper Series
New Conditions and Constellations in Cyber

Contra: The Incidents at Sea Agreement is a Poor Model for Cyberspace

Benjamin Bahney | Senior Fellow, Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR)
Jonathan Reiber | Senior Director for Cybersecurity Strategy and Policy, AttackIQ
Brandon Williams | Cybersecurity postdoctoral Fellow,Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR)

December 2021

Tensions between the major powers have risen significantly in recent years, and cybersecurity matters have been some of the key flash points. The U.S. has long perceived that China has fueled its economy and military rise by stealing intellectual property, and the Russian government interfered in the 2016 U.S. elections using disinformation and influence operations in cyberspace. Conversely, Russia and China have expressed consternation about U.S. "left of launch" and Stuxnet-like capabilities that threaten their infrastructure and their strategic forces.[1,2] Reciprocal concerns have been widespread over quotidian hacking, interference, and in some cases destruction of private-sector data and systems.

U.S. Government responses to these challenges have run the gamut. U.S. policymakers have indicted foreign military operators for cybertheft, treating these incidents as traditional espionage, and analysts suspect that in other cases the U.S. has undertaken reciprocal responses where the behavior was more injurious.[3] But the policy community also seeks new diplomatic solutions. A 2014 bilateral agreement between Presidents Obama and Xi Jinping attempted to reduce cy-

Benjamin Bahney is a Senior Fellow at Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR) where he studies strategic competition in the 21st century in the areas of space, cyber, and advanced science and technology.

Jonathan Reiber is Senior Director for Cybersecurity Strategy and Policy at AttackIQ, where he leads the company's narrative and content creation programs and directs key strategic issues. During the Obama administration he served as Speechwriter and Chief Strategy Officer for Cyber Policy in the Office of the Secretary of Defense

Dr. Brandon Kirk Williams is a cybersecurity postdoctoral fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory. His research focuses on the intersection of cybersecurity, emerging technology, and national security policy.

bersecurity tensions by proscribing states conducting intellectual property theft in cyberspace for commercial gains, and by establishing new track 1.5 groups to work on cyberspace law enforcement and military stability issues. But tensions around cyberspace issues have only risen since 2014, and arms control proponents seek additional rules of the road and consultative mechanisms to build stronger adherence to international law and norms and to create new channels of engagement between militaries and diplomats.

In our analysis the idea of an INCSEA for cyberspace fails to be relevant to today's security environment on three key counts: it does not match the political conditions between the major powers, it does not fit the operational realities of the cyberspace domain, and it does not address the key policy challenges and stability challenges related to cybersecurity.

At first blush, a cyberspace agreement that emulates the 1972 incidents at sea (INCSEA) agreement—which built similar mechanisms for the high seas once the Soviets established a blue water Navy—seems like a plausible avenue toward stabilizing military cyberspace affairs. However, in our analysis the idea of an INCSEA for cyberspace fails to be relevant to today's security environment on three key counts: it does not match the political conditions between the major powers, it does not fit the operational realities of the cyberspace domain, and it does not address the key policy challenges and stability challenges related to cybersecurity. To make these points, first we will lay out the INCSEA agreement in historical context to understand the conditions leading to its promulgation and the problems it solved. Second, we will analyze the INCSEA concept in the face of the operational realties and policy problems in the cyberspace domain, and third we will discuss how it falls short of addressing the key problems of the cyberspace domain today.

The Agreement between the U.S. Government and the Government of the Russian Federation on the Prevention of Incidents On and Over the High Seas was signed on May 25, 1972, by Secretary of the Navy John Warner and the Soviet Union's Commander in Chief of the Navy Sergei Gorshkov. Commonly referred to as INCSEA, the bilateral agreement binds both parties to stated rules for the conduct of each country's ships and airplanes on and over the high seas to reduce the risk of escalation.[4]

INCSEA established a code of conduct for transparency, non-interference, information sharing, advanced notice of activity, and annual consultations, as well as an agreement to avoid threatening activity. INCSEA built on previous international agreements—such as the 1958 Geneva Convention of the High Seas—that codified rules for the operation of military and civilian vessels on and above the high seas. INCSEA does not restrain limits on force size, exercises, or the operation of each nation's navy or air force.

Representatives from the United States and Russia meet annually on a bilateral basis to reaffirm INCSEA and to discuss its application of ship-to-ship and air-to-air contact during the previous year. The consultations preserve INCSEA's continuity and place it in a suite of important bilateral confidence building measures originating in the relaxation of Cold War superpower tension in the early 1970s period of détente.

President Lyndon Johnson's administration exchanged the first diplomatic notes with the Soviet Union that ultimately culminated in INCSEA's 1972 signing at a high tide of superpower diplomacy. Informal bilateral discussions between the navies began in 1966, but a worrying crescendo of near

misses in 1968 convinced the Departments of State and Defense to amplify requests for a formal agreement. A TU-16 bomber, in one instance, crashed in May 1968 after buzzing U.S. ships operating in the Norwegian Sea, raising the risk of collisions that could spiral into escalation. Undersecretary of State Nicholas Katzenbach wrote Deputy Secretary of Defense Paul Nitze in 1968 warning him of the risks and an ostensible lack of interest from the Soviet Union. Overtures throughout 1968 from the U.S. Departments of State and Defense to Soviet counterparts went unanswered until the climate of superpower relations improved.[5]

Henry Kissinger notified Richard Nixon that the impasse broke in 1971 after Soviet diplomats formally requested consultations on incidents at sea. The president approved Kissinger's request to proceed with formal dialogue and consolidate the effort in the hands of the National Security Council in place of overlapping formal and private conversations.[6] "We seem to be enjoying something like an 'era of good feeling'," the United States' ambassador to Russia reported after productive deliberations between the two superpowers on incidents at sea. Forward progress on a future INCSEA occurred, however, only in the context of Détente's thaw.[7]

The Soviet Union and the United States signed INCSEA during a 1972 summit in Moscow when Nixon and Soviet Premier Leonid Brezhnev signed the Strategic Arms Limitation Treaty. In preparation for the state visit, Kissinger alerted Nixon that a raft of agreements on disparate subjects were slated for announcement: space, the environment, health, science and technology, commerce, and incidents at sea. Both parties formalized INCSEA amidst a rewiring of the frayed bilateral circuits to resume conversations on traditional state-to-state matters.[8]

INCSEA and the decades of annual consultations improved the condition of naval security and strategic stability for approximately fifty years. It ensured safety of navigation on and over the high seas even during instances of heightened tension, provided commanders with stated rules, created the bilateral machinery for dialogue, and reduced the opportunity for pilot or captain miscalculation. By the mid-1980s, troubling episodes on and above the high seas had declined markedly, and INCSEA served as evidence of a successful confidence-building measure.

The relationships between the three major cyberspace powers today—namely, the U.S., China and Russia—are far more contentious than what was present during the period of détente leading up to the INCSEA agreement.

INCSEA, ultimately, was a product of a specific historical moment when two competing powers mutually agreed to diminish the strategic, tactical, and accidental escalatory catalysts. Senior leaders in the United States and the Soviet Union recognized that competition could occur without risky conduct below the threshold of war. Confidence-building measures governing visible objects and domains, such as the high seas, proved easier to implement. Policymakers in Washington and Moscow mutually agreed that they benefited by reducing tension, and a transparent code of conduct on the high seas was one lever by which to restore stability for bilateral relations and geopolitics.

However, the political conditions that led to INCSEA are largely missing today. While there is a movement toward some agreement on normative measures in the United Nations, the required political conditions are much broader than that. The relationships between the three major cyberspace powers today—namely, the U.S., China and Russia—are far more contentious than what was present during the period of détente leading up to the INCSEA agreement. There is no common view between the powers on how cyberspace relates to strategic stability, which was a clear

precursor to INCSEA. There is also no clear motivation by the major powers to explore new arms control measures for cyberspace, and no shared drive to tamp down tensions as there was in the late 1960s and early 1970s after the U.S. and the Soviet Union had come close to the brink during the Cuban Missile Crisis in 1962.

Today's arms control environment, rather, is one where we see significant backsliding with major treaties having been recently jettisoned, such as the Anti-Ballistic missile treaty, the Intermediate Nuclear Forces Treaty, and the Open Skies Treaty. Rather than cooperation and threat reduction, the major powers appear to be in a mindset of unbridled competition—more akin to the 1950s and early 1960s when we saw significant international crises, and when arms control seemed far off into the future. But surely, political conditions could change in the wake of a major crisis, or given significant changes in the leadership of the major power states. So if these conditions do change, could INCSEA address the fundamental realities and challenges of cyberspace competition?

Not really. The reasons are three-fold.

First, cyberspace operations occur in cyberspace via a network of data centers, servers, routers, switches, computers, and devices owned by private and government entities in sovereign territory—and there is no similar consensus upon the existence of an equivalent of the "high seas" in cyberspace. Even if operators conceal their locations, they are always operating in sovereign territory on someone's network. Damage, disruption, or theft done to data on a network therefore impacts a specific data owner or operator, and is a violation of sovereignty.

Second, while cyberspace operators might "bump into" each other on the infrastructure if they are both present on a network—two intruders passing in the night, as it were—these are virtual interactions and seem unlikely to cause inadvertent material harm in the same way that navies could do so on the high seas. The intruder would need to manipulate data and cause material and irreversible harm for it to be analogous, in some way, to two ships colliding on the open seas. Similarly, there would need to be some risk that an incident of cyberspace operators bumping into each other could rise to the level of an armed attack under international law, via the irreversible destruction of life or property, if it were to plausibly carry a significant risk of escalating to war. This is an unlikely occurrence in cyberspace.

Third and most importantly, if the United States and Russia or China are to have productive conversations about cyberspace, the most important issue is for the states to make progress on adhering to bounds of acceptable state behavior in peacetime and conflict. This is a far greater legal and policy challenge for the bilateral relationship, and an INCSEA-like agreement is wholly irrelevant to its resolution.

Cyberspace is a new arena of operations. Over the last decade, as access has increased exponentially across the globe, adversaries have flourished in the "gray space" below the level of outright conflict that cyberspace affords, escalating their operations against the United States without fear of real retribution. That is how China has stolen U.S. intellectual property through cyberspace with impunity, why North Korea broke into and damaged Sony Pictures Entertainment's networks before the release of the parody film The Interview, and why the Russian Federation conducts cyber-enabled disinformation operations in advance of U.S. elections, penetrates U.S. critical infrastructure, and sows seeds of social discord within the U.S. population. For more than a decade, revisionist nation states have exploited the vulnerabilities that cyberspace affords. Countries have conducted hostile operations online, through disinformation and cyberspace operations, without

ever having to leave their home, with limited resource investments, recognizing that the United States was not entirely sure how best to respond.

For years the United States largely held back against each of the above actors, not wanting to trigger a tit-for-tat response in cyberspace that could escalate. Instead, the United States sought to impose retributive costs through indictments and sanctions. This did not help achieve deterrence in cyberspace. But perhaps the Russian government's interference in the 2016 U.S. Presidential election was a watershed moment. In 2018, the United States military gained the authority with which to conduct cyberspace operations to stop cyberattackers in advance of attacks against core U.S. interests, an expression of the new U.S. strategy to "defend forward" in cyberspace.[9] This suggests that, if the United States has indicators and warning of a potential cyberattack against its vital interests—such as its critical infrastructure—as it did in advance of the 2018 elections, the United States may take action to defend American interests online. Outside of the U.S. military's use of operations in cyberspace, following a spike in ransomware attacks in 2020 and 2021 against hospitals and infrastructure, the U.S. Department of Justice targeted cybercriminals by seizing their bitcoin holdings,[10] and the U.S. Treasury Department implemented sanctions on the global malware market by targeting cryptocurrency instruments.[11]

The goal of this increasingly forceful response posture is to help set and assert the bounds of acceptable behavior, along with deterring hostile activities, to include countries that allow ransomware operators to conduct criminal activities without fear of arrest. The Russian government's actions in the SolarWinds intrusion and in allowing ransomware groups to flourish within its borders remains a pre-eminent concern in matters of policy and law for the United States in cyberspace. This problem cannot be addressed through an INCSEA-like agreement because the principal issue is that the Russian government allows malicious cyberspace operators in its territory to act with impunity.

If there is any place for legal agreements in matters of cybersecurity, diplomacy should occur around the question of how to set and maintain responsible state behavior in cyberspace.

If there is any place for legal agreements in matters of cybersecurity, diplomacy should occur around the question of how to set and maintain responsible state behavior in cyberspace. The cybersecurity community has made progress here in multilateral fora. Concurrent with the United States increasing its efforts to deter and disrupt attacks on its interests, the United Nations countries have built on decades of work from the UN's cybersecurity Group of Governmental Experts (GGE) to affirm the need for norms of operations in cyberspace, such as refraining from targeting medical devices or other critical infrastructure.[12] But unlike with INCSEA, these multilateral agreements do not seem to have curtailed Russian malign influence operations in cyberspace.

Bilaterally, the U.S. and Russia put in place emergency communications during the Obama administration to tamp down the chance of conflict spiraling out of control. Increasing communication about strategic capabilities is certainly to the good, and that might be what has urged the call for an INCSEA-like treaty: to discuss and shape how forces operate. But the United States can pursue those discussions through existing lines of communication around norms and crisis management.

The analogies of an INCSEA treaty otherwise fail to demand a new direction for U.S. policy and law. Recall that the original INCSEA treaty established rules of the road for maneuvering military weapon platforms (and later, merchant marine ships as well) to include the use of flag communications between vessels. At times these frightening close maritime engagements involved nuclear

weapon platforms such as strategic missile submarines and bombers. INCSEA also set rules of the road for the use of weapon engagement threats such as the opening of bomb bay doors on bombers that are nearby ships, the use of fire control radars against other vehicles or vessels, and simulated attacks.

For these two conditions, there is clearly no analogue yet in cyberspace. There is no record of threatening engagements between military cyberspace operators of one country and the strategic platforms or weapon systems of another, nor do we know of equivalent "dangerous maneuvers" in cyberspace that could put either side at risk. Last, there is no clear way to brandish weapons threats from cyberspace operators against specific weapons systems or platforms. Cyberspace operators do not seem to saddle up to one another and show off their malware in a chat room to threaten the other side. The absence of these conditions makes it unlikely today that cyberspace operations could result in inadvertent nuclear escalation, or that cyberspace operators could scare strategic weapons operators and their chain of command into using their weapons.

The absence of these conditions makes it unlikely today that cyberspace operations could result in inadvertent nuclear escalation, or that cyberspace operators could scare strategic weapons operators and their chain of command into using their weapons.

For these reasons, it is doubtful that an INCSEA-like agreement for cyberspace would be germane to the security concerns of today's cyberspace competition, that it could tamp down strategic tensions between states, or that such an agreement could be practicable.

The INCSEA treaty of 1972 was clearly a product of a period when the major powers sought détente and a reduction in tensions, and incidents on the high seas—outside of sovereign waters—between military combatants in peacetime were a potential vehicle to accidental or inadvertent escalation between nuclear armed states. There is no relevant mapping of this historical context to the political situation in 2021, nor does the situation in maritime affairs in the late 1960s and early 1970s have any relevance to cyberspace operations today. While the political conditions for such agreements could change rapidly given a change in geopolitics, it is hard to imagine how the strategic and operational context of military competition in cyberspace could approximate the maritime context of the period.

The views and opinions of the authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, Inc. LLNL-JRNL-829171

Endnotes

1 Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations," Brookings Institution, February 2012. https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf

2 Vladamir Radyuhin, "Stuxnet could have created Chernobyls: Russia," The Hindu, January 27, 2011. https://www.thehindu.com/news/international/Stuxnet-could-have-created-Chernobyls-Russia/article15535416.ece

3 Julien Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," New York Times, Oct 23, 2018. https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html

4 "Agreement Between the Government of The United States of America and the Government of The Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas," conclusion date: May 25, 1972, U.S. Department of State, https://2009-2017.state.gov/t/isn/4791.htm .

5 Nicholas Katzenbach, "Letter From the Under Secretary of State (Katzenbach) to the Deputy Secretary of Defense (Nitze)," Foreign Relations of the United States (FRUS), 1964-1968, Volume XIV, Soviet Union, Document 284, August 16, 1968. https://history.state.gov/historicaldocuments/frus1964-68v14/d284

6 Henry Kissinger, "Memorandum From the President's Assistant for National Security Affairs (Kissinger) to President Nixon," FRUS, 1969-1976, Volume XIII, Soviet Union, Document 113, February 16, 1971. https://history.state.gov/historicaldocuments/frus1969-76v13/d113

7 U.S. Embassy in the Soviet Union, "Telegram From the Embassy in the Soviet Union to the Department of State," FRUS, 1969-1976, Volume XIV, Soviet Union, Document 7, October 22, 1971. https://history.state.gov/historicaldocuments/frus1969-76v14/d7

8 Henry Kissinger, "Memorandum From the President's Assistant for National Security Affairs (Kissinger) to President Nixon," FRUS, 1969-1976, Volume XIV, Soviet Union, Document 227, May 15, 1972. https://history.state.gov/historicaldocuments/frus1969-76v14/d227

9 US CYBERCOM, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," US CYBERCOM website, April 2018. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

10 U.S. Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," U.S. Department of Justice, June 7, 2021, available at https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

11 U.S. Department of the Treasury, "Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group," U.S. Department of the Treasury Office of Public Affairs, March 2, 2021, available at https://home.treasury.gov/news/press-releases/sm924

12 Josh Gold, "Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?," CFR Blog, March 2021, https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what

About the Authors

Benjamin Bahney is a Senior Fellow at Lawrence Livermore National Laboratory's Center for Global Security Research (CGSR) where he studies strategic competition in the 21st century in the areas of space, cyber, and advanced science and technology. His research is focused on how these new areas of competition alter strategic stability, deterrence, and escalation management. Also as the laboratory's Space Program leader, he oversees all work on both space science and space security. Ben has written for Foreign Affairs magazine, Foreign Policy, Lawfare, War on the Rocks, and has contributed to the opinion pages of the New York Times. Ben was a contributor to the U.S. Cyberspace Solarium Commission, particularly on public private partnerships. He was also a contributor to the edited volume Cross-Domain Deterrence: Strategy in an Era of Complexity published by Oxford University Press (2019). Ben was formerly an analyst at the RAND Corporation.

Jonathan Reiber is Senior Director for Cybersecurity Strategy and Policy at AttackIQ, where he leads the company's narrative and content creation programs and directs key strategic issues. During the Obama administration he served as Speechwriter and Chief Strategy Officer for Cyber Policy in the Office of the Secretary of Defense, where he authored the first two national cyberdefense strategies of the United States. His commentary has appeared in TIME Magazine, Foreign Policy, Lawfare, and The Atlantic Monthly and his research has been supported by the Smith Richardson Foundation, Watson Foundation, and Berkeley's Center for Long-Term Cybersecurity. He is the author of A Public, Private War, the findings of which were adopted by the U.S. Cybersecurity Solarium Commission and the National Defense Authorization Act of 2021. He is a graduate of Middlebury College and The Fletcher School.

Dr. Brandon Kirk Williams is a cybersecurity postdoctoral fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory. His research focuses on the intersection of cybersecurity, emerging technology, and national security policy. His work addresses geopolitical competition and alliances in the Indo-Pacific and has been published in Lawfare and CGSR reports on Indo-Pacific Cybersecurity, strategy and emerging technology, and strategic competition with China. He earned a PhD in history from the University of California, Berkeley, where he completed a dissertation examining national security history that was supported by a Fulbright-Hays Grant for research in Indonesia.

Cyberstability Paper Series
New Conditions and Constellations in Cyber

Pro: Transposing the Incidents at Sea Agreement – A Thought Experiment

Alexander Klimburg, PhD* | Director, Global Commission on the Stability of Cyberspace and Secretariat

December 2021

A lack of agreed signaling protocols nearly led to World War Three. On October 27, 1962, at the height of the Cuban Missile Crisis, the US Navy cornered one of the few Soviet submarines unaccounted for off the coast of Cuba. In an effort to convince the FOXTROTT-class sub B-59 to surface, the destroyer USS Cony employed practice depth charges—which, however, were not accurately identified as such by the beleaguered crew. When the sub did indeed surface and engaged in communication, an anti-submarine aircraft flew low over the sub and dropped flares and pyrotechnics. This convinced the captain of the sub to crash drive, and, according to the detailed account in the 2020 book *Nuclear Folly,* a vigorous debate ensued on board the ship as to whether this constituted an attack, and the order was given to fire the sub's nuclear torpedoes, each with 10 Kiloton warheads, at the US navy task force. It was only in the last moment that the fire order was rescinded.

The 1972 Incident at Sea Agreement (INCSEA) was a milestone in de-escalation and confidence building. In clear and concise language, it created rules for a number of possible scenarios where Soviet and American navy forces might meet on the high seas—such as that which occurred during the Cuban Missile Crisis, where misunderstandings over signaling nearly led to an apocalypse. The success of INCSEA did not come lightly. By the time it was signed, ten years after the

* For the pro/contra article series the author reclused himself from his role as editor and reviewer of the Cyber Stability Paper series, and did not see the opposing article in advance.

Alexander Klimburg is the Director of the Global Commission on the Stability of Cyberspace Initiative and Secretariat, and the Director of the Cyber Policy and Resilience Program at The Hague Centre for Strategic Studies. He is also a Senior Associate at the Center for Strategic and International Studies (CSIS) and an Associate Fellow at the Austrian Institute of European and Security Policy.

incident described above, the rapidly expanding Soviet and US Navies were increasingly bumping into each other—often enough literally. The potential for "inadvertent escalation"—i.e., accidental war—was obvious. Agreed-upon norms were clearly needed. However, it still took both sides nearly four years to negotiate the agreement after the US first proposed it. But it was worth it; although the Cold War would go on to thaw and freeze and thaw again, the military-to-military agreements held sound, and prevented something worse from happening. In 1983, Secretary of the Navy John Lehman cited the accord as "a good example of functional navy-to-navy process" and credited this area of Soviet-American relations with "getting better rather than worse." In 1985, he observed that the frequency of incidents was "way down from what it was in the 1960s and early 1970s." This was despite a much-expanded navy on both sides.

The success of INCSEA has often been remarked upon when considering possible agreements in dealing with escalating cyber tensions today—after all, "disentangling" forces in cyberspace may seem like a practical and useful step in order to avoid serious accidents. Indeed, if anything, the scope of misunderstandings in cyberspace is even larger then that between navies during the Cuban Missile Crises: the realities of the domain mean that, for instance, it can be difficult for a cyber defender to differentiate between a malicious act as an attempt at espionage or as preparation for an act of war. INCSEA is not the only such agreement from which to draw, and the 1989 Prevention of Dangerous Military Activities Agreement[2] has some very promising cyber-adaptable aspects as well, as we shall see later.

But INCSEA is often evoked as the main model for a potential operational cyber agreement.[3] Detractors to the INCSEA-for-cyber (INCSEA-C) model sometimes like to point out that sea and cyber domains are not mirror images of each other. This is true, but the differences should not be overemphasized. All domains are unique, and it is the commonalties that need to be considered in a transposition, not the differences. The challenge, for instance, of establishing definitive attribution also exists at sea, and both planes and especially submarines are not always clearly identifiable.[4] And, as with navy forces, cyber forces have to "navigate" a domain that is often not bound by territorial sovereignty, and must consider civilian traffic as well.

The position of the United States (and most of the like-minded group of liberal democracies) over the last decade has been to avoid any formal political agreement on cyber conflict, for at least four good reasons: Firstly, most potential terms in cyber "treaties" were considered to be unverifiable, and would lead only to rampant cheating (or the expectations of such) and thus would prompt even more instability. Secondly, the implication that current International Law was not sufficient would create a precedent to open up other areas to new negotiation. Thirdly, any treaties on cyberspace would imply that states were the ultimate arbiter of the entire domain, conflicting with the Western position of a nonstate-led Internet. Fourthly, Russia has persistently led China and others in trying to equate what they view as psychological information warfare with technical cyberattacks. Effectively, this has amounted to focusing on means to protect what they call their "Internet segment" from content they consider destabilizing. When in September 2020 Russia's President Putin offered to negotiate with the United States on INCSEA-for-cyber,[5] these four points were clearly apparent, and he added a fifth reason to refuse such an offer: not giving Russia the status of a peer with the United Sates in a bilateral agreement, something undeniably politically important to Vladimir Putin. As a result, the Russian INCSEA-C offer was largely and understandably dismissed by US and Western commentators.[6]

Even though the INCSEA-for-cyber as a bilateral US–Russian agreement may be out of the question for the moment, there are good reasons why an INCSEA-C could be considered in a differ-

ent, multilateral format, although not on the basis of the Russian September 2020 proposal. For instance, it could be considered as a new Confidence Building Measure within the Organization of Security and Cooperation in Europe (OSCE, although China would be absent), or even as a Memorandum of Understanding appended to existing UN First Committee initiatives. For the four basic reasons that like-minded democracies tend to (rightly) refuse cyber agreements do not apply here: "disentangling cyber" does not require counting cyber forces or even clear attribution of actual "attacks," so the first concern of cheating leading to escalation is largely mute. If cast as an agreement (let alone as a Confidence Building Measure or Memorandum of Understanding), it would not be a "treaty" in that it would create new international law,[7] but quite the opposite (as we shall see below), it can reinforce existing law—so the second concern would be mute. Regarding the third concern on undermining the nonstate-led Internet governance model: the focus is only on proscribing state behavior, so with correct wording this danger could be avoided as well. And regarding the fourth concern—not equating psychological-effect actions such as propaganda and covert influencing with the use of force and armed attack—this has been a cornerstone of international law for decades, and should not be reversed, despite recent Western military's considerations of responding to disinformation with kinetic-equivalent operations as a counter measure under international law. This precondition admittedly would likely be the largest stumbling block in getting the process off the ground.

Even though the INCSEA-for-cyber as a bilateral US–Russian agreement may be out of the question for the moment, there are good reasons why an INCSEA-C could be considered in a different, multilateral format, although not on the basis of the Russian September 2020 proposal.

But if all this were possible, that would leave the final, perhaps most important, question: what would an INCSEA-for-cyber actually do? What would it look like? This is where the efficacy of the original INCSEA agreement comes into play, where the military negotiators crafted a bare-bones agreement on three pages and with five articles of agreement.[8] As a thought experiment, it is an interesting challenge to transpose the document directly to cyber, although, immediately, some transpositions are easier than others.

For instance, Article I of the INCSEA would already seem a stumbling block. In the original document, definitions of "ship," "aircraft," and "formations" are agreed upon—and only in 122 words. This would undoubtedly be trickier for INCSEA-C; while the Internet, computers and networks might be easy to define, the stumbling block cyber/information/data "weapon" could be huge. The solution? Do not refer to weapons, but rather to possible effects (such as "interfering with..") that are technologically independent. A similar track has been taken with the current norms of restraint put forward in the UN First Committee processes.

Article II of INCSEA directly references and invokes the "International Regulations for Preventing Collisions at Sea" (later called COLREGs), a set of agreements under the International Maritime Organization that are commonly referred to in the document as "Rules of the Road." Veteran watchers of the UN First Committee Processes will remember that the eleven norms agreed upon in the 4th Group of Governmental Experts (GGE) Report[9] are often described as "rules of the road." In both cases, the intent was to reinforce existing international law while explicitly spelling out nonbinding and voluntary norms of behavior. The same principle could apply for Article 2 in an INCSEA-C: a clear commitment to the UN General Assembly-endorsed eleven norms would

provide both a common point of departure while reinforce existing international law. Just like the COLREGs outlined in 1972, the eleven GGE norms would represent a "common language" on specific behavior that is partially only further spelled out in the INCSEA-C. The importance of this common baseline is critical; one criticism of a similar bilateral military agreement between China and the United States is that it has largely failed due to a lack of common rules of the road being spelled out.[10]

Article III of INCSEA focuses on "hazardous actions and maneuvers," and a number of ideas are remarkably pertinent for a transposition to cyber. For instance, Article III paragraph 6 directly says that the Parties should "not simulate attacks," by aiming guns or such, at each other. One of the most significant challenges in cyber is that some activities do not seem to have other functions (such as intelligence gathering) and are either a clear threat of the use of force, or even a case of advanced preparation of the battlefield. For instance, leave-behinds (large encrypted files) in critical infrastructure networks without any meaningful raw intelligence value can often only be interpreted as a preparation for attack. Often enough, activities observed, e.g., in the power grid meet this case, and sometimes the attacker may even draw attention to their existence by a cyber "shot across the bow" that may be excessively escalatory. In the same paragraph 6, another interesting parallel can be found, namely "not using searchlights or other powerful illumination devices to illuminate the navigation of bridges of passing ships." The reason for this is obviously one of blinding the crew and thus imperiling ship navigation. A near parallel for this could actually be "excessive" or malicious port and network scanning activities. While port and network scanning are regular and should be considered part of the background noise of the Internet, excessive or malicious port scanning, such as shining a blinding light into a ship's pilot's eyes, can cause a defender undue concern that a serious attack is coming. It can even directly affect some network activity. Speaking of affecting network activity, paragraph 3 explicitly excludes navy ships from conducting maneuvers through areas of heavy traffic. Something similar could be said about an injunction of governments prohibiting the conducting of training (or offensive peacetime operations) that unduly infringes upon the availability or integrity of civilian services.

Often enough, activities observed, e.g., in the power grid meet this case, and sometimes the attacker may even draw attention to their existence by a cyber "shot across the bow" that may be excessively escalatory.

One of the most intriguing parallels to be drawn in Article III is, however, paragraph 4. It reads "ships engaged in surveillance of other ships…avoid executing maneuvers embarrassing or endangering the ships under surveillance."[11] In seaman's terms, "embarrassing another ship" means causing it to take evasive actions in a way that may endanger it or others. There is a case to be made that there is such a thing as "cyber embarrassment": a case where the surveilling actor causes the defending actor to undertake actions damaging to itself or others. If, for instance, a cyber espionage case is so severe that, e.g., a foreign ministry is forced to disconnect itself from the Internet to attempt to clean up the attack, this "cyber maneuver" would cause significant follow-on effects, such as, for instance, citizens in urgent need of help would not be able to contact their representatives. This example is made even more poignant in purely civilian cases, such as when emergency or 911 numbers and similar numbers are affected. This author has speculated on what cases of cyber-espionage could potentially rise to the level of a threat or the actuality of use-of-force,[12] and more recently law scholars have also started to opine on the matter.[13] The notion of a "cyber embarrassment" is therefore a potentially rich field for deliberation that easily exceeds this short essay.

Article IV of INCSEA concentrates on the hazardous maneuvering of aircraft over ships. But it provides a useful point of departure for a cyber version to concentrate on something similarly connected to one domain but part of another—and that is security of communication links, in particular those of undersea cables and satellite. While nations have always considered spying on communication cables (and satellites) to be a justified activity in peacetime, some limitations may be reasonable if there is a reasonable chance that the availability or integrity of civilian services could be affected. This would include any kind of interference that interrupts the communication completely, such as, for instance, by inadvertently cutting a cable while tapping it, or a poorly-designed cyber espionage attack on a satellite or ground station that renders the system temporarily inoperable. While these infrastructures are already indirectly covered in international law as well as the 4th and 6th UN GGE Report, they have not been previously explicitly mentioned. This would also be a great opportunity to directly address the security of the global undersea cable infrastructure overall, also highlighting that implied conventional threats carried out with loitering with naval vessels (as occurred in 2015, 2018, and recently in 2021[14]) would be out of bounds as well. Artful wording in this paragraph would even be able to address yet another increasingly problematic issue, namely, one of wideband GPS jamming, which has led to a number of naval incidents as of late.[15] Ideally, a separate Article could even be considered binding all parties to non-interference in the availability of integrity of the basic backbone infrastructure of the global Internet. A norm proposed by the Global Commission on the Stability of Cyberspace (GCSC) on the non-interference with this so-called "public core" could provide a baseline; indeed, much of the spirit of the GCSC's work was already adopted in the reports of the 2021 Open-Ended Working Group and GGE.

There is a case to be made that there is such a thing as "cyber embarrassment": a case where the surveilling actor causes the defending actor to undertake actions damaging to itself or others.

This Article could also allow the introduction of a category of protection found in a different mil-mil agreement, namely the "Special Caution Areas" (SCAs) mentioned in the 1991 Prevention of Dangerous Military Activities Agreement.[16] SCAs are defined by each party in mutual agreement, and have special protective measures assigned to them. For instance, an SCA could include the dedicated nuclear command and control infrastructure of a country,[17] and the activity in question could be a prohibition on all kinds of cyber activity in this SCA to avoid any appearances that these capabilities were to be preemptively eliminated. SCAs could also, however, include a number of civilian infrastructures, including large Internet Exchange Points and others. Indeed, the aforementioned "public core of the Internet" infrastructure would represent an easy SCA to which all could likely agree.

The remaining Articles address the exchange of information, both operationally at sea as well as strategically, between military staffs reviewing the agreement. In cyber terms there have been repeat efforts to instigate similar communication protocols, both at the operational and political (but not at the in-between strategic) levels, but they often have been inconclusive. The most common operational approach has been to identify national technical points of contact[18] on the defender side (national CERTs or equivalent). Most of these arrangements (with notable exceptions such as CBM 8 of the OSCE[19]) miss a crucial element: an escalation ladder in case of non-responsiveness, going up to the political level, such as, for example, to a responsible cabinet minister, if necessary.[20] Further, there are few (if any) such regular strategic exchanges between actual cyber commands or similar entities that are responsible for offensive cyber operations. A "cyberhotline" can be described as a political level tool, and, if used without support from regular links established on the

strategic level, can potentially be a dead end, as seen in the 2016 US Presidential Election.[21] Equally important, therefore, are multiple direct international links between leading officials and officers in cyber policy. Finally, there is no process yet within the multilateral space by which to have a closed emergency consultation on cyber issues—there is no "in between" forum between a closed emergency UN Security Council meeting and bilateral or public exchanges, such as the confidential network the OSCE tries to provide to its participating states.[22] This means that there is a lack of options by which states may properly signal to each other that there is a crises, potentially leading to a state of public re-criminations and loss of escalation control.

Overall, the success and failure of such an agreement would largely depend on the sophistication of those negotiating it, and it would require some time, until the political will has been adequately mobilized.

In conclusion, it may need to be stressed that any good agreement would require sacrifices on both sides. There are points in the above thought-experiment that might be difficult for members of the like-minded group of liberal democracies to accept, and there are certainly points that would be difficult for Russia and China to accept as well. It will only be feasible if those responsible think that such an agreement will have more benefits then costs—and it is very obvious that costs and benefits (the equites) are not being assessed equally across and between governments. The situation is further complicated by the reality that the two main ideological blocks in cyber have fundamentally different priorities in what they want from these discussions—the United States and the like-minded group may be worried about "cyber war," but Russia and China are certainly more concerned with what they think is "Information war."[23] The INCSEA-C thought experiment is clearly orientated toward the former concern. Overall, the success and failure of such an agreement would largely depend on the sophistication of those negotiating it, and it would require some time, until the political will has been adequately mobilized. However, as we have seen over recent years, the political will and intent on cyber issues has gyrated widely, often depending on serious cyber incidents to set the agenda. Smart policy making will be aware of the threat of allowing the news headlines to dictate the conversation, and would be well advised not only to react, but to get ahead of the curve. Thinking seriously about a multilateral Incident at Sea for the Cyber model is a good step in regaining the initiative.

Endnotes

1 "Agreement Between the Government of The United States of America and the Government of The Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas," conclusion date: May 25, 1972, U.S. Department of State, https://2009-2017.state.gov-/t/isn/4791.htm

2 "Prevention of Dangerous Military Activities Agreement," WikiSource, last modified July 16, 2019, https://en.wikisource.org/wiki/Prevention_of_Dangerous_Military_Activities_Agreement.

3 This includes also by representatives of the United States State Department.

4 Attribution is remarkably similar in places—when claiming infringements of an air defense identification zone, common practice of states was not to require technical evidence (such as radar pictures)—for the same reasons that attribution of cyber attacks are often done without presenting technical data.

5 Tom Balmforth and Anton Kolodyazhnyy, "Putin says Russia and U.S. should agree not to meddle in each other's elections," Reuters, September 25, 2020, https://www.reuters.com/article/uk-russia-usa-putin-idUKKCN26G1OM

6 For instance, see Greg Austin and Alexander Stronell, "Why Putin's call for a US–Russia cyber reset will fall on deaf ears," The International Institute for Strategic Studies, October 1, 2020, https://www.iiss.org/blogs/analysis/2020/09/csfc-putins-cyber-reset. However, it needs to be pointed out that a former senior US Department of State representative stated that he and his colleagues had raised the idea of the INCSEA-C themselves in a multilateral context before, and the US government overall has been open to this idea in the past.

7 The majority view of scholars is that the original INCSEA is still considered as an "agreement," not a "treaty"—while the signing parties clearly define it as an agreement (e.g., not creating international law, and not requiring ratification by the US Senate), this might change with time, as other states adapt it as common practice.

8 See Takuya Shimodaira, "Chapter 7. Measures to Enhance Maritime Safety—Expansion of Code for Unplanned Encounters at Sea (CUES) Exercise," International Symposium on Security Affairs 2017 by the National Institute for Defense Studies (July 2017), http://www.nids.mod.go.jp/english/event/symposium/pdf/2017/e-07.pdf

9 United Nations Group of Governmental Experts, "Group of Governmental Experts on Developments in the
Field of Information and Telecommunications in the Context of International Security," United Nations, July 22, 2015, https://undocs.org/A/70/174

10 This is the Military Maritime Consultative Agreement (MMCA) of 1998. For a critique, see Shimodaira, "Chapter 7. Measures to Enhance Maritime Safety", http://www.nids.mod.go.jp/english/event/symposium/pdf/2017/e-07.pdf

11 "Agreement Between the Government of The United States of America and the Government of The Union of Soviet Socialist Republics on the Prevention of Incidents On and Over the High Seas," Article III, paragraph 4.

12 Alexander Klimburg, The Darkening Web: The War for Cyberspace, (New York: Penguin Books, 2017).

13 Duncan B. Hollis and Tsvetelina van Benthem, "What Would Happen If States Started Looking at Cyber Operations as a 'Threat' to Use Force?," Lawfare, March 30, 2021, https://www.lawfareblog.com/what-would-happen-if-states-started-looking-cyber-operations-threat-use-force

14 H. I. Sutton, "Russian Spy Ship Yantar Loitering Near Trans-Atlantic Internet Cables," Naval News, August 19, 2021, https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yan-

tar-loitering-near-trans-atlantic-internet-cables/ and "Concern over Russian ships lurking around vital undersea cables," CBS News, March 30, 2018, https://www.cbsnews.com/news/russian-ships-undersea-cables-concern-vladimir-putin-yantar-ship/

15 Gareth Corfield, "Russia spoofed AIS data to fake British warship's course days before Crimea guns showdown," The Register, June 14, 2021, https://www.theregister.com/2021/06/24/russia_ais_spoofing/

16 "Prevention of Dangerous Military Activities Agreement," WikiSource, https://en.wikisource.org/wiki/Prevention_of_Dangerous_Military_Activities_Agreement

17 This is notwithstanding some claims by US analysts that some nuclear powers may have "purposely entangled" their conventional and nuclear C&C structure to prevent them from being targeted. Even if true, it is irrelevant—using the example of the DMAA, an SCA may only be agreed by all parties, not declared unilaterally.

18 One of these is the MERIDIAN Group Contact List, although this does include China and Russia.

19 Organization for Security and Co-operation in Europe Permanent Council, "Decision No. 1202 OSCE Confidence-Building Measures To Reduce The Risks Of Conflict Stemming From The Use Of Information And Communication Technologies," Organization for Security and Co-operation in Europe, March 10, 2016, https://www.osce.org/files/f/documents/d/a/227281.pdf

20 A similar "contact escalation ladder" is implied in Confidence Building Measure 2 of the OSCE list. See, Organization for Security and Co-operation in Europe Permanent Council, "Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies,".. This author proposed that component in the OSCE 1039 working group, and justified it with the experience of the China–Japan–Korea Memorandum of Understanding that utilized this approach.

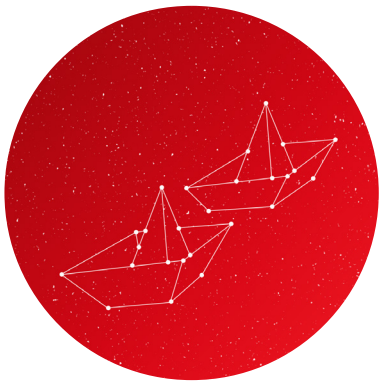
21 The US–Russia "cyber hotline" was set up in 2013 on the basis of the famous nuclear "hot line," but was only used once, in 2016, to little effect. Erin Banco and Kevin Poulsen, "This Hotline Could Keep the U.S. and Russia From Cyberwar," The Daily Beast, March 07, 2019, https://www.thedailybeast.com/this-hotline-could-keep-the-us-and-russia-from-cyber-war

22 The OSCE Network is a secure, closed network that can send messages bilaterally but also to groups. Thomas Greminger, "Vienna Cyber Security Week—Protecting Critical Infrastructure—Opening remarks," Organization for Security and Co-Operation in Europe, March 11, 2019, https://www.osce.org/files/f/documents/9/7/415007.pdf

23 Alexander Klimburg, The Darkening Web: The War for Cyberspace, (New York: Penguin Books, 2017)

About the Author

Dr. Alexander Klimburg is Director of the Global Commission on the Stability of Cyberspace Initiative and Secretariat and Director of the Cyber Policy and Resilience Program at The Hague Centre for Strategic Studies. He is an Affiliate and former Fellow at Harvard University, and an associate fellow at the Austrian Institute of European and Security Policy. Alexander Klimburg has worked on numerous topics within the wider field of international cybersecurity. He has acted as an adviser to a number of governments and international organizations on national cybersecurity strategies, international norms of behavior in cyberspace and cyber-conflict (including war, cyber-crime, and cyber-espionage), critical infrastructure protection, and internet governance. He has participated in international and intergovernmental discussions within the European Union and the Organization for Security and Co-operation in Europe and has been a member of various national, international, NATO, and EU policy and working groups. He has given dozens of invited talks and regularly participates and organizes track 1.5 diplomatic initiatives as well as technical research groups. He is author and editor of numerous books, research papers, and commentaries and has often been featured in the international media, including in Newsweek, Reuters, and others. His most recent book The Darkening Web: The War for Cyberspace was published by Penguin Press.



About the Cyberstability Paper Series

Since the release of the final report of the Global Commission on the Stability of Cyberspace in November 2019, the concept of cyberstability has continued to evolve. A number of new 'conditions' are emerging: new agreements on norms, capacity building and other stability measures have been proposed and solidified within the United Nations and elsewhere, and stakeholders are exploring ways to increase stability and minimize the risk of conflict in cyberspace through technical fixes or governance structures. The constellations of initiatives involved in working towards cyberstability is expanding, underlining the need to connect the traditional state-led dialogues with those of the Internet communities from civil society and industry. Gaps continue to close, between the global north and south, between technology and policy, but also the stability in and the stability of cyberspace.

The first Cyberstability Paper Series explores these "New Conditions and Constellations in Cyber" by collecting twelve papers from leading experts, each providing a glance into past or future challenges and contributions to cyberstability. The papers are released on a rolling basis from July until December 2021, culminating in an edited volume. All papers will be available for open access, and a limited number of printed hardback copies are available.

Published by

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

The Hague Centre
for Strategic Studies