SEPTEMBER 2022

Of Ships and Cyber

Transposing the Incidents at Sea Agreement

By Alexander Klimburg

Amid the geopolitical crises caused by Russia's February 2022 invasion of Ukraine, it may seem wildly optimistic—or even bad diplomacy—to consider future arms-control scenarios for cyber operations. However, good policy needs to prepare for the day after tomorrow, and smart policy will look at what has gone wrong today and what can be learned from yesterday. Arguably, one element that may have contributed to rising geopolitical tensions over the past decade has been a lack of clear cyber signals among the main adversaries. This makes it even more urgent to consider what can be learned from past arms-control exercises such as the vaunted Incidents at Sea (INCSEA) Agreement—especially as this accord was conceived in the wake of several of its own perilous crises.

In 1962, a lack of agreed signaling protocols nearly led to World War III. According to a riveting account in the 2020 book *Nuclear Folly*,[1] on October 27, 1962—at the height of the Cuban Missile Crisis—the U.S. Navy cornered one of the few Soviet submarines unaccounted for off Cuba. In an effort to convince the Foxtrot-class *B-59* submarine to surface, the destroyer USS *Cony* employed practice depth charges—which were not accurately identified as such by *B-59*'s beleaguered crew. When, in the middle of the night, the submarine did indeed surface, a low-flying anti-submarine aircraft dropped flares and pyrotechnics so it could take better photographs. This seemed like an attack to the submarine, and the exhausted captain of *B-59* ordered a crash dive and speculated that perhaps the war had already broken out. He gave orders to prepare to launch a 10-kiloton nuclear torpedo at the U.S. Navy task force. It took a near-mutiny by senior officers to stop him.

This close call remained unknown until fairly recently. But several more prominent naval incidents throughout 1960s convinced the Soviet Union and the United States that a basic common agreement was necessary, and the Cold War "thaw" of the early 1970s made this possible.

1. Serhii Plokhy, *Nuclear Folly: A History of the Cuban Missile Crisis* (New York: W. W. Norton & Company, 2021), 266–72.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

The 1972 INCSEA was a milestone in de-escalation and confidence building. In clear and concise language, it created rules for numerous possible scenarios where Soviet and U.S. naval forces might meet on the high seas. The success of INCSEA did not come lightly. By the time it was signed, the rapidly expanding Soviet and U.S. navies were increasingly bumping into each other—sometimes literally. The potential for "inadvertent escalation" (i.e., accidental war), was obvious. Agreed-upon norms of behavior were clearly needed. It took both sides nearly four years to negotiate the agreement after the United States first proposed it. But it was worth it: Although the Cold War continued to thaw and freeze and thaw again, the military-to-military agreements held sound and prevented worse from happening. In a U.S. State Department reference in the agreement, "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'," despite a much-expanded navy on both sides.

The success of INCSEA has often been remarked upon when considering possible agreements for 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 than between navies during the Cuban Missile Crisis. The realities of the domain mean that it can be difficult, for instance, for a cyber defender to categorize a malicious act as an attempt at espionage or preparation for an act of war. INCSEA is not the only such agreement to draw from, and the 1989 Prevention of Dangerous Military Activities Agreement (PDMAA) has some very promising cyber-adaptable aspects as well. But INCSEA is often evoked as the main model for a potential operational cyber agreement, including by representatives of the U.S. Department of State. Detractors of the INCSEA-for-cyber (INCSEA-C) model sometimes 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 instead the commonalties that should be considered in a transposition. The challenge of establishing definitive attribution also exists at sea, and planes and submarines are not always clearly identifiable.[2] And, like navy forces, cyber forces have to "navigate" a domain often not bound by territorial sovereignty, as well as to consider civilian traffic.

> *The success of INCSEA has often been remarked upon when considering possible agreements for 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.*

The position of the United States (and most like-minded liberal democracies) over the past decade has been to avoid any formal political agreement on cyber conflict, for at least four good reasons. First, 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. Second, the implication that current international law was not sufficient would create a precedent to open other areas to new negotiation. Third, any treaties on cyberspace would imply that states were the ultimate arbiter of the entire domain, conflicting with the Western position of a non-state-led internet. Fourth, Russia has

2. Attribution is remarkably similar in places—for instance, when claiming infringements of an air-defense identification zone, states' common practice was not to require technical evidence such as radar pictures—for the same reasons that attribution of cyberattacks are often carried out without presenting technical data.

persistently led China and others in trying to equate what it views as psychological information warfare with technical cyberattacks. Effectively, this has amounted to focusing on the means to protect what it calls its "internet segment" from content it considers destabilizing. When Russian president Vladimir Putin offered to **negotiate** with the United States on an INCSEA-C in September 2020, not only were these four points apparent, he inadvertently provided a fifth reason to refuse the offer: not giving Russia the status of a peer with the United Sates in a bilateral agreement, something undeniably politically important to Putin. As a result, U.S. and Western commentators largely and **understandably dismissed** the Russian INCSEA-C offer. However, a former senior U.S. Department of State representative stated that he and his colleagues had raised the idea of INCSEA-C themselves in a multilateral context before, and the U.S. government overall has seemed open to this idea in the past.

Even though INCSEA-C as a bilateral U.S.-Russian agreement may be out of the question for the moment, there are good reasons why an INCSEA-C could be applied to a different, multilateral format. For instance, it could become a confidence-building measure (CBM) within the Organization of Security and Cooperation in Europe (OSCE), although China would be absent, or even a memorandum of understanding (MOU) appended to existing UN First Committee initiatives. This is because the four basic reasons like-minded democracies tend to (rightly) refuse cyber agreements do not apply here. "Disentangling cyber" does not require counting cyber forces or even a clear attribution of actual "attacks," so the first concern that cheating leads to escalation is largely mute. If cast as an agreement (let alone as a CBM or MOU) it would not be a "treaty" that creates new international law[3]—indeed, it might do quite the opposite (as discussed below) and reinforce existing law—so the second concern would be moot. Regarding the third concern that it would undermine the non-state-led internet-governance model, the focus is only on proscribing state behavior, so with correct wording this danger could be avoided as well. And the fourth concern—not equating psychological-effect actions such as propaganda and covert influencing with use of force and armed attack—has been a cornerstone of international law for decades and should not be reversed, despite recent Western militaries considering responding to disinformation with kinetic-equivalent operations as a countermeasure. This precondition admittedly would likely be the largest stumbling block in getting the process off the ground.

But if all this were possible, this leaves the final, perhaps most important, question: What would an INCSEA-C actually do? This is where the efficacy of the original INCSEA, where the military negotiators crafted a bare-bones **agreement** of five pages and 10 articles, helps show the way. As a thought experiment, it is an interesting challenge to transpose the document directly to cyberspace—though some transpositions will initially be easier than others.

For instance, Article I of INCSEA appears to be a stumbling block. In the original document, definitions of "ship," "aircraft," and "formation" are agreed upon—and in only 122 words. This would undoubtedly be trickier for INCSEA-C. While the "internet," "computers," and "networks" might be easy to establish, defining cyber, information, or data "weapons" could be difficult. The solution? Do not refer to weapons, but rather to possible effects (such as "interfering with . . .") that are technologically independent. The current norms of restraint put forward in the UN First Committee processes follow a similar track.

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

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

commonly referred to in the document as "rules of the road." Veteran watchers of the UN First Committee processes will remember that the 11 norms agreed upon in the fourth Group of Governmental Experts (GGE) report are often described as "rules of the road" as well. In both cases, the intent was to reinforce existing international law while explicitly spelling out nonbinding and voluntary norms. The

same principle could apply to Article II in an INCSEA-C: A clear commitment to the 11 norms endorsed by the UN General Assembly would both provide a common point of departure and reinforce existing international law. Just like the COLREGs outlined in 1972, the 11 GGE norms would represent a common language on specific behavior that is only partially further spelled out in INCSEA-C. This common baseline is vital: One criticism of a similar bilateral military agreement between China and the United States, the Military Maritime Consultative Agreement (MMCA) of 1998, is that it has struggled due to a lack of common rules of the road being spelled out.[4]

> *The same principle could apply to Article II in an INCSEA-C: A clear commitment to the 11 norms endorsed by the UN General Assembly would both provide a common point of departure and reinforce existing international law.*

Article III of INCSEA, which focuses on "hazardous actions and maneuvers," contains several ideas that are remarkably pertinent for a transposition to cyberspace. For instance, the sixth paragraph says the parties to the agreement should "not simulate attacks" (e.g., aim guns at each other). One of the most significant challenges in cyber policy is that it can be difficult to assess the internet behind cyber operations: What may be intended solely as an intelligence gathering operation may appear to be a preparation of the battlefield or even actual imminent attack. For instance, leave-behinds (which can include backdoors or but also in particular encrypted files) inserted into critical infrastructure networks can often only be interpreted as a preparation for attack, especially if these networks have no meaningful raw intelligence value. When enough such activities are observed—such as in the power grid—the attacker may draw attention to their existence in a cyber "warning shot across the bow" that may be excessively escalatory. In the same paragraph, another interesting parallel can be found, namely not using "searchlights or other powerful illumination devices to illuminate the navigation bridges of passing ships"—obviously to avoid blinding the crew and thus imperiling ship navigation. A near parallel for this could 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, like shining a blinding light into a ship 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, the third paragraph explicitly excludes navy ships from conducting maneuvers in areas of heavy traffic. Something similar could ban governments from conducting training (or offensive peacetime operations) that unduly infringes on the availability or integrity of civilian services.

However, one of the most intriguing parallels to be drawn from Article III is in the fourth paragraph. It reads, "Ships engaged in surveillance of other ships . . . shall avoid executing maneuvers embarrassing or

4. For a critique see, for example, Takuya Shimodaira, "Measures to Enhance Maritime Safety: Expansion of Code for Unplanned Encounters at Sea (CUES) Exercise," in *Maintaining Maritime Order in the Asia-Pacific* (Tokyo: The National Institute for Defense Studies, 2018), 113–31, http://www.nids.mod.go.jp/english/event/symposium/pdf/2017/e-07.pdf.

endangering the ships under surveillance." In seaman's terms, "embarrassing another ship" means causing it to take evasive actions in a way that might endanger it or others. There is a case to be made that there is such a thing as a "cyber embarrassment" wherein the surveilling actor causes the defending actor to undertake actions damaging to itself or others. If, for instance, a cyber espionage case were so severe that a foreign ministry needed to disconnect itself from the internet to attempt to clean up the attack, this "cyber maneuver" would cause significant follow-on effects, such as leaving citizens in urgent need of consular help unable to contact their representatives. Alternately, a hospital might be forced to take some critical systems offline to deal with a cyber intrusion, leading to a noticeable increase of deaths due to administrative errors. Both of these examples are not fiction: they have occurred, as have similar incidents, several different times in the past. This author has previously speculated on what cases of cyber espionage could potentially rise to the level of threat or actuality of use-of-force.[5] More recently, legal scholars have also started to opine on the matter; 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 hazardous maneuvering of aircraft over ships. But it provides a useful point of departure for a cyber version to concentrate on the security of communication links, in particular those of undersea cables and satellites, which are something similarly connected to one domain but part of another. While nations have always considered spying on communication cables and satellites to be a justified activity in peacetime, some limitations are reasonable if the availability or integrity of civilian services could inadvertently be affected. This would include any kind of interference that interrupts the communication completely, such as by accidentally damaging 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 fourth and sixth UN GGE reports, they have not previously been explicitly mentioned. This would also be a great opportunity to directly address the security of the global undersea cable infrastructure overall, highlighting that implied conventional threats carried out by loitering naval vessels (as occurred in 2015, 2018, and 2021) 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 Global Positioning System (GPS) jamming, which has led to several recent naval incidents. Ideally, a separate article could even bind all parties to noninterference in the availability or integrity of the internet's basic backbone infrastructure. One possible baseline could be a norm proposed by the Global Commission on the Stability of Cyberspace (GCSC) on the noninterference in the "public core of the internet;" indeed, much of the spirt of the GCSC's work in this regard has already been adopted in the reports of the GGE and the 2021 UN Open-ended Working Group on cybersecurity.

Such an article could also allow the introduction of a category of protection found in a different military-to-military accord, the "special caution areas" (SCAs) mentioned in the 1989 PDMAA. SCAs are defined by each party in mutual agreement and have special protective measures assigned to them. For example, an SCA could include a country's dedicated nuclear command-and-control infrastructure, and the article could prohibit all kinds of cyber activity in this SCA to avoid any appearances that these capabilities are being targeted.[6] SCAs could also include a number of civilian infrastructures, including large internet exchange points or the name servers that underpin the functioning of the Domain Name System. Indeed, the

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

6. This is notwithstanding some claims by U.S. analysts that certain nuclear powers may have "purposely entangled" their conventional and nuclear command-and-control structure to prevent them from being targeted. Even if true, it is irrelevant: Using the example of the PDMAA, an SCA only be agreed by all parties, not declared unilaterally.

infrastructure of the aforementioned "public core of the internet" would represent an easy SCA to which all could likely agree. The PDMAA Annexes also features a number of detailed signaling agreements (including radio frequencies to use and phrases to be mentioned) that also could easily be adapted to a cyber INCSEA.

The remaining articles of INCSEA managed the exchange of information, both operationally (at sea) and strategically (between military staffs reviewing the agreement). In cyber terms, there have been repeated efforts to instigate similar communication protocols, both at the operational and political (though 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 on the defender side—national computer emergency response teams or the equivalent.[7] Most of these arrangements—with notable exceptions such as CBM 8 of OSCE Permanent Council Decision No. 1039—miss a crucial element: a communication escalation ladder in case of non-responsiveness, going up to the political level, say a responsible cabinet minister.[8] Further, there are few (if any) such regular strategic-level exchanges between actual cyber commands or similar entities that are responsible for offensive cyber operations. A "cyber hotline" can be described as a political-level tool, but if used without support from regular links established on the strategic level, it can potentially be a dead end, as seen in the U.S. attempts to use it to warn off Russian interference in the 2016 U.S. presidential election. Equally important are multiple, direct, multilateral exchanges among leading officials and officers in cyber policy. There is currently no process yet within the multilateral space to have an open emergency consultation on cyber issues—i.e., there is no intermediate forum between a closed, emergency UN Security Council meeting and bilateral or public exchanges such as the secure communication network the OSCE provides its participating states.[9] This means there is a lack of options for states to properly signal to each other in a crisis, potentially leading to public recriminations and loss of escalation control.

> *Most of these arrangements [national technical points of contact]—with notable exceptions such as CBM 8 of OSCE Permanent Council Decision No. 1039—miss a crucial element: a communication escalation ladder in case of non-responsiveness, going up to the political level, say a responsible cabinet minister.*

In conclusion, any good agreement requires sacrifices on both sides. There are points in the thought experiment above 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 as well. It will only be feasible if those responsible think that such an agreement will have more benefits than costs—and it is obvious that costs and benefits 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 policy have

7. One of these is Meridian Group International's contact list, although this does include entities in China and Russia.

8. A similar "contact escalation ladder" is implied in CBM 2 of the OSCE list. See Organization for Security and Cooperation 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," PC Journal No. 1092, agenda item 1, March 10, 2016, https://www.osce.org/files/f/documents/d/a/227281.pdf. This author proposed that component in the OSCE 1039 working group and justified it with the experience of the China-Japan-Korea MOU that utilized this approach.

9. The NATO-Russia Council (NRC) can be viewed as a political, not strategic level tool—mostly orientated toward building cooperation in areas such as on cooperation in Afghanistan but did not include cyber.

fundamentally different priorities for these discussions. The United States and like-minded democracies may be worried about "cyber warfare," but Russia and China are certainly more concerned with what they define as "information warfare."[10] The INCSEA-C thought experiment is clearly oriented 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 enough political will has been mobilized. However, as seen over recent years, the political will and intent regarding cyber issues have fluctuated widely, often depending on serious cyber incidents to set the agenda. Smart policymakers will be aware of the risk of allowing news headlines to dictate the conversation and would be well advised to not only react but also get ahead of the curve. Thinking seriously about a multilateral INCSEA model for cyber policy is a good step toward regaining the initiative. ■

Alexander Klimburg *is a senior associate (non-resident) in the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

10. Klimburg, *The Darkening Web*, 15.