sipri

SIPRI Insights on Peace and Security

No. 2023/10 November 2023

MAPPING CYBER-RELATED MISSILE AND SATELLITE INCIDENTS AND CONFIDENCE-BUILDING MEASURES

LORA SAALMAN, LARISA SAVELEVA DOVGAL AND FEI SU

SUMMARY

● Cyber incidents that—whether due to human error, system malfunction or intentional targeting—impact satellite and missile systems extend beyond the ongoing war in Ukraine. These systems are essential to civilian and military operations and disrupting them has the potential to elicit conventional or even nuclear retaliation. Due to the centrality of satellite and missile-related infrastructure, cyber incidents impacting the functionality of such infrastructure have served as a catalyst for previous confidence-building measures (CBMs) that may provide a template for future ones. This paper builds on SIPRI work to map cyber-related missile and satellite incidents, as well as unilateral, bilateral and multilateral CBMs to provide takeaways meant to foster greater predictability and stability in cyberspace.

I. Introduction

Cyber incidents impacting satellite infrastructure and triggering false missile alarms have become integral parts of the war in Ukraine.[1] These incidents are escalatory because missile and satellite systems are essential to civilian and military operations and have the potential to elicit conventional or even nuclear retaliation. Such targeting of civilian and military infrastructure promises to amplify not only as combat continues but also within future conflicts. Cyber-related incidents that compromise missile and satellite infrastructure—whether due to human error, system malfunction or intentional targeting—not only have a lengthy history, but also have served as an impetus for the building of confidence-building measures (CBMs) in relation to such incidents.[2] To better understand these dynamics, this SIPRI Insights Paper maps cyber-related missile and satellite incidents and CBMs.[3] While always evolving, this mapping can be useful in both evaluating past and present CBMs and informing new ones, since consensus is often generated through locating commonly faced threats and potential catalysts for escalation.

This paper builds upon SIPRI's findings on cyber postures and cyber incidents from recent publications and workshops related to China, the European Union (EU), Russia and the United States.[4] Section II outlines

[1] The term 'cyber' is used to refer to activities, processes and systems 'involving the use of a computer'. Collins Dictionary, Definition of 'cyber', [n.d.]; Erwin, S., 'Cyber warfare gets real for satellite operators', *SpaceNews*, 20 Mar. 2022; Barrett, A., 'False alarms, true dangers? Current and future risks of inadvertent US–Russian nuclear war', RAND Corporation, 2016; and Archon, 'Cyber concerns for the satellite sector', [n.d.].

[2] See various fact sheets at Arms Control Association, 'Fact sheets: Missiles and missile defense', Arms Control Association, [n.d.]; see also Sampson, V. and Weeden, B., 'Enhancing space security: Time for legally binding measures', *Arms Control Today*, Dec. 2020.

[3] CBMs may be defined as 'measures that address, prevent, or resolve uncertainties among states', which can be 'formal or informal, unilateral, bilateral, or multilateral, military or political, and can be state-to-state or non-governmental'. Center for Strategic and International Studies, 'Confidence-building measures', [n.d.].

[4] While the European Union represents a body comprised of member states, for the purposes of this project, it is being treated as a unitary actor, with the policies of individual member states highlighted when they distinguish themselves from the collective. Saalman, L., Su, F. and Saveleva Dovgal, L., 'Cyber crossover and its escalatory risks for Europe', SIPRI Insights on Peace and Security no. 2023/9, Sep. 2023; Saalman, L., Su, F. and Saveleva Dovgal, L., 'Cyber posture trends in China, Russia, the United States and the European Union', SIPRI, Dec. 2022; SIPRI, 'SIPRI

publicly available cases of cyber-related missile and satellite incidents, covering inadvertent errors as well as deliberate targeting. Section III uses these cases as a foundation to trace unilateral, bilateral and multilateral CBMs related to cyber incidents involving missile and satellite infrastructure. Section IV concludes with a brief overview of how the trends identified can be a first step for policy makers in facilitating predictability and stability in cyberspace.

II. Cyber-related missile and satellite incidents

Cyber incidents such as those that have compromised Viasat satellite operations in Ukraine and triggered false missile alerts in Russia are not unique to the war in Ukraine. There have been numerous cyber-related missile and satellite incidents resulting from human error, system malfunction and intentional targeting that date back to the 1960s. Based on information that is publicly available, and recognizing the limitations of research based on open sources, the cases outlined in this section were selected for the alleged involvement of computers in incidents that carried either the threat of destruction or kinetic response, whether from attempted control, disruption or destruction of satellite systems or false alarms of missile attacks. They are described in terms of each category of cause—human error, system malfunction and intentional targeting—and in chronological order within those categories.

Incidents caused by human error

1962: Moorestown missile false alarm

In October 1962 radar operators in Moorestown, New Jersey informed a national command post that a nuclear attack appeared to be underway. The false alarm came from a test tape being run that simulated a missile launch from Cuba, while a satellite simultaneously came over the horizon, confusing the operators. This led them to notify North American Aerospace Defense Command (NORAD) of an anticipated nuclear strike. During the incident, overlapping radars that should have confirmed or denied the attack were not in operation.[5]

1979: Exercise tape insertion and false missile warning

In November 1979 a technician mistakenly inserted an exercise tape for training purposes into a computer running the US early-warning programs at NORAD, causing the computer to broadcast warnings of an incoming Soviet nuclear strike against US nuclear command centres. Launch control centres for Minuteman intercontinental ballistic missiles (ICBMs) received a preliminary warning that the USA was under nuclear attack and the continental air defence interceptor force was put on alert, with at least 10 fighters

hosts workshop on cyber incidents and threat perceptions', News and events, 16 July 2023; SIPRI, 'SIPRI co-hosts workshop with ORF America on cyber postures and dynamics', News and events, 16 Nov. 2022; and SIPRI, 'Cyber postures and dynamics: China, Russia, United States and Europe', Workshop, SIPRI and the Observer Research Foundation America, Washington, DC, 2–3 Nov. 2022.

[5] Phillips, A., '20 mishaps that might have started accidental nuclear war', Nuclear Age Peace Foundation, 15 Jan. 1998.

taking off. The officers reviewed the raw data from the Defense Support Program satellites and checked with the early-warning radars, determining that there were no signs of attack, so the alert was cancelled.[6]

2018: Hawaii false missile alert

In January 2018 Hawaiian residents received a text message sent by the Hawaii Emergency Management Agency with a false alert stating: 'Ballistic missile threat inbound to Hawaii. Seek immediate shelter. This is not a drill.' This message was revoked 38 minutes after it was issued, in the wake of confusion and panic. The mistake occurred during a shift-change drill that takes place three times a day at the emergency command post, according to a spokesman for the agency. Officials said the alert was the result of human error and not the work of hackers or a foreign government.[7]

Incidents caused by system malfunction

1980: Typographical computer errors and false missile warning

In 1980 three false alarms occurred in May and June. This was due in part to a faulty integrated circuit and a faulty message design in NORAD computers, leading to a computer at NORAD generating typographical errors in the routine messages it sent to Strategic Air Command (SAC) and the National Military Command Center. While the message typically read '000' ICBMs or submarine-launched ballistic missiles (SLBMs) had been launched, some of the zeroes were replaced with a two—for example, '002' or '200'—so the messages instead read that two, then 200, SLBMs were en route. The randomness of the numbers prompted a review of the data, which determined there were no incoming missiles.[8]

1983: Oko early-warning system malfunction

In September 1983 the Soviet early-warning satellite system called Oko malfunctioned, with alarms alerting the base of a small number of incoming ICBMs. While light and sound alarms were activated, signalling an incoming nuclear attack, some officers on duty were sceptical that the USA would launch only a few ICBMs. Oko was reportedly prone to error, in this case thought to have been caused by the glint of the sun on the satellite due to its angle and positioning. Rather than immediately alerting superiors up the chain of command, one of the duty officers awaited corroborating evidence from the ground echelon of the early-warning system, which never came, and the alarms eventually stopped.[9]

[6] National Security Archive, 'False warnings of Soviet missile attacks put US Forces on alert in 1979–1980', 16 Mar. 2020; and United States Space Force, 'Defense Support Program satellites', Fact sheet, Oct. 2020.

[7] Nagourney, A., Sanger, D. E. and Barr, J., 'Hawaii panics after alert about incoming missile is sent in error', *New York Times*, 13 Jan. 2018.

[8] Forden, G., 'False alarms on the nuclear front', *NOVA Online*, Oct. 2001.

[9] Center for Arms Control and Non-proliferation, 'The Soviet false alarm incident and Able Archer 83', 14 Oct. 2022; National Park Service, 'Stanislav Petrov', [n.d.]; and Дворкин, В. [Dvorkin, V.], Ядерное сдерживание: концепции и риски [Nuclear deterrence: Concepts and risks], Мировая экономика и международные отношения [*World Economy and International Relations*], 2019, vol. 63, no. 12.

2010: Computer hardware failure at Warren Air Force Base

In October 2010 the US Air Force was unable to communicate with or monitor 50 of the 319th Missile Squadron's Minuteman III ICBMs. The breakdown reportedly appeared to be caused by a hardware failure, during which five computers went 'out of sync'. Multiple error codes were reported, including 'launch facility down'. During an approximately 45-minute window, the computers were shut down and rebooted. This meant that during this time the ICBMs were not launchable, including by the airborne back-up system.[10]

Incidents caused by intentional targeting

1997/1998: ROSAT satellite failure

In late 1997 an allegedly Russian hacker used social engineering and a dictionary attack—respectively, psychological manipulation and a preselected library of passwords—to access internet-connected file transfer protocol servers located on the mission computer network of the National Aeronautics and Space Administration (NASA). Within this network, the Goddard Space Flight Center server managed files associated with the joint US, German and United Kingdom X-ray satellite Röntgensatellit's (ROSAT) command-and-control systems. The breach potentially contributed to the systems' miscalculation of the satellite's alignment, turning it towards the sun and causing it to overheat. While NASA corrected for what it believed to be system error, a few months later in 1998 the hacker reportedly changed the attitude-control system code, causing the satellite to again point its imager towards the sun, this time irreparably damaging it.[11]

2018: US satellite network infiltration

In June 2018 Symantec identified the advanced persistent threat (APT) group Thrip and three computers based in China as having breached satellite operators, defence contractors and telecommunications companies in the USA and Southeast Asia. Symantec alleged that the APT group seemed to focus on the operational side of the satellite operator impacted, looking for and infecting computers running software that monitors and controls satellites, potentially with the aim of disruption.[12]

2022: Viasat KA-SAT cyberattack

In February 2022 a destructive denial-of-service (DDoS) cyberattack was used to push the AcidRain destructive wiper against Viasat's KA-SAT network. The cyberattack impacted several thousand customers located in Ukraine and tens of thousands of other fixed-broadband customers across Europe, including approximately 3000 wind turbines in Germany. This incident was localized to a single consumer-oriented partition of the

[10] Shachtman, N., 'Communication with 50 nuke missiles dropped in ICBM snafu', *Wired*, 26 Oct. 2010; and NBC News, 'Glitch disrupts Air Force nuke communications', 7 Oct. 2010.

[11] Wess, M., 'ASAT goes cyber', *Proceedings of the US Naval Institute*, vol. 147, no. 2 (2021); and Tucker, P., 'The NSA is studying satellite hacking', *Defense One*, 20 Sep. 2019.

[12] Symantec, 'Thrip: Espionage group hits satellite, telecoms, and defense companies', Threat Intelligence Blog, 19 June 2019.

KA-SAT network that is operated on Viasat's behalf by a Eutelsat subsidiary, Skylogic.[13]

2022: Cyberattacks and missile strikes against infrastructure in Ukraine

In March 2022 Ukrainian media companies based in Kyiv faced destructive attacks and data exfiltration, alongside missile strikes against a television tower on the same day. In the wake of destructive cyberattacks on government computer networks, missile and artillery strikes assailed Vinnytsia airport and government buildings in Dnipro. These activities were accompanied first by similar efforts to undertake cyber intrusions to compromise computer systems, then by physical occupation of a Ukrainian nuclear power plant. In the months that followed, other power plants also suffered physical occupation and close-proximity missile strikes.[14]

2022: Roscosmos satellite compromise

In March 2022 Network Battalion 65 (NB65), reportedly linked to the Anonymous hacker group, claimed to have stolen data from Roscosmos—a government corporation that oversees the Russian space industry. In doing so, NB65 shared a tweet allegedly containing Russian space agency's WS02 Vehicle Monitoring System server information. Roscosmos did confirm that there were attempts to break into their control centre. However, while the NB65 reportedly succeeded in exfiltrating documents and administration materials, evidence does not yet suggest that they gained access to Roscosmos' operational systems.[15]

2022: Starlink jamming and disruption

In March 2022 SpaceX's Starlink satellite in low Earth orbit experienced 'signal jamming' in user terminals in Ukraine. In November 2022 Starlink also suffered a DDoS attack from KillNet that made the service inaccessible for several hours. Unrelated to these incidents, Starlink was also reportedly targeted by a computer simulation developed by China's Northwest Institute of Nuclear Technology, a People's Liberation Army (PLA) research institute, to evaluate nuclear anti-satellite weapon performance at different altitudes and yields. This included the ability of a 10-megaton nuclear blast 50 miles from the Earth's surface to disable Starlink satellites passing through the radioactive cloud.[16]

[13] Viasat, 'KA-SAT network cyber attack overview', 30 Mar. 2022; and Guerrero-Saade, J. A., 'AcidRain: A modem wiper rains down on Europe', Sentinel One, 31 Mar. 2022.

[14] Microsoft Digital Security Unit, 'An overview of Russia's cyberattack activity in Ukraine', Special Report: Ukraine, 27 Apr. 2022, pp. 8, 14; 'Chernobyl power plant captured by Russian forces: Ukrainian official', Reuters, 25 Feb. 2022; and 'Russian missile strikes close to nuclear plant, Ukraine says', PBS News Hour, 19 Sep. 2022.

[15] 'Рогозин рассказал о предотвращении атак хакеров на ЦУП и спутники' [Rogozin spoke about preventing hacker attacks on the control center and satellites], Известия [*Izvestiya*], 2 Mar. 2022; Anonymous TV (@YourAnonTV), Twitter, 1 Mar. 2022, <https://twitter.com/YourAnonTV/status/1498792639877074945?lang=en>; Johnson, B., 'Anonymous vs. Russia: Hackers say space agency breached, more than 1,500 websites hit', 1 Mar. 2022; and Bender, B., 'Russia's space chief says hacking satellites "a cause for war"', *Politico*, 2 Mar. 2022.

[16] Malik, T., 'Elon Musk says SpaceX focusing on cyber defense after Starlink signals jammed near Ukraine conflict areas', Space.com, 5 Mar. 2022; and Chen, S., 'Chinese physicists simulate nuclear blast against satellites', *South China Morning Post*, 20 Oct. 2022.

Table 1. Cyber-related missile and satellite incidents, 1962–2023

Year	Human error	System malfunction	Intentional targeting
1962	Moorestown missile false alarm		
1979	Exercise tape insertion and false missile warning		
1980		Typographical computer errors and false missile reading	
1983		Oko early-warning radar malfunction	
1997/98			ROSAT satellite failure
2010		Computer hardware failure at Warren Air Force Base	
2018	Hawaii false missile alert		US satellite network infiltration
2022			Viasat KA-SAT cyberattack Cyberattacks and missile strikes on infrastructure in Ukraine Roscosmos satellite compromise Starlink jamming and disruption
2023			Russian media false missile alerts Dozor-Teleport cyberattack

2023: Russian media false missile alerts

In February 2023 Russian radio stations played a loud siren sound with a message announcing: ‘Everyone go to the shelters immediately. Attention! Attention! Threat of a missile strike’, throughout the cities of Belgorod, Stary Oskol, Ufa, Kazan, Novouralsk, Novosibirsk, Pyatigorsk, Tyumen, Voronezh, Nizhny Novgorod and Magnitogorsk, as well as a number of districts of Moscow. A cyberattack on the infrastructure of a satellite operator was reportedly behind the false alarm, according to Russia’s Ministry of Emergency Situations.[17]

2023: Dozor-Teleport cyberattack

In June 2023 hackers claimed to be behind the failure of satellite systems and destruction of information on servers of Dozor-Teleport—one of the leading Russian satellite telecommunications providers that services power lines and oil fields, in addition to Russian Defence Ministry military units, the Federal Security Service, the pension fund, Russia’s northern merchant fleet and the Bilibino nuclear power plant. The hackers also claimed to have defaced four Russian websites with messaging supportive of the Wagner Group—a private military company allegedly supported by the Russian government—and released a link to a zip file containing 674 files. While some Russian experts have claimed that this was likely a false flag operation, at least two entities claimed responsibility for the cyberattacks, one describing itself as a hacktivist group and the other as part of the Wagner Group.[18]

[17] ‘Hacking attack prompts Russian regional broadcasters to issue air alert warnings’, Reuters, 28 Feb. 2023; and Glover, C., ‘Russian radio stations hacked with bogus missile warning from hacktivists’, *TechMonitor*, 23 Feb. 2023.

[18] Vicens, A. and Vasquez, C., ‘Hackers attack Russian satellite telecom provider, claim affiliation with Wagner Group’, *CyberScoop*, 29 June 2023; Menn, J., ‘Cyberattack knocks out satellite communications for Russian military’, *Washington Post*, 30 June 2023; Лепехина, Е. [Lepekhina, E.], ‘Хакеры, связывающие себя с ЧВК «Вагнер», заявили об атаке на провайдера «Дозор-Телепорт». Он обслуживает российские госкорпорации’ [Hackers associated with the Wagner PMC announced an attack on the Dozor-Teleport provider. It services Russian state corporations], RTVI, 30 June 2023; and ‘Кибератака на «Дозор-Телепорт»: кто и зачем взломал оператора спутниковой связи’

Mapping of cyber-related missile and satellite incidents

Table 1 shows the above incidents mapped on a chronological timeline against each category of cause: human error, system malfunction and intentional targeting. While acknowledging that unreported cases likely occurred, table 1 nevertheless suggests a trend towards intentional targeting of missile and satellite infrastructure since 2018. Whereas much of this may relate to the war in Ukraine, the success of such cyberattacks on and off the battlefield indicates how such tactics may be employed in future conflicts. In particular, the deliberate targeting of critical infrastructure related to civilian services raises questions as to how the private sector is to be identified and treated in the context of war.[19] Whether through cyber targeting of satellites that provide civilian and military communications, as occurring in Ukraine, or through cyber targeting of media services to spread fears of missile attacks, as occurring in Russia, these trends merit greater attention for their potential foundation for CBMs, as discussed in the next section.

III. Cyber-related missile and satellite CBMs

The above-listed cyber-related missile and satellite incidents have had a catalytic impact on not just escalation through conventional or even nuclear retaliation, but also on the development of CBMs relevant to the incidents. This section provides an overview of various unilateral, bilateral and multilateral measures to inform discussion of cyber-related CBMs. CBMs are voluntary and enable a state to assess its vulnerabilities, threats and remediation strategies, which are crucial aspects of sharing information with allies for cooperation and with adversaries to reduce misunderstandings. While the cases described and mapped in section II were not the only factors shaping the CBMs outlined in this section, they contributed to the urgency surrounding the formulation of these measures. The CBMs described below are organized under the categories of unilateral, bilateral and multilateral and then mapped by category along the timeline.

Unilateral CBMs

Retaining human control and mitigating computer error

Following the false missile warning caused by computer error in 1980, an adviser to the US president stressed that similar malfunctions may ‘someday generate another false alert’, such that ‘we must continue to place our confidence in the human element of our missile attack warning system’.[20] Since that time, particularly within the field of artificial intelligence (AI), the USA has increasingly prioritized human control, reflected most recently in its 2022 Nuclear Posture Review and a February 2023 declaration that states

[Cyberattack on Dozor-Teleport: Who hacked the satellite operator and why], SecurityLab.ru, 5 Oct. 2023.

[19] Christery, V., ‘ICRC statement on existing and potential threats in the sphere of information security’, Statement at the fourth substantive meeting of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, New York, 6 Mar. 2023.

[20] US National Security Archive, ‘The 3 a.m. phone call: False warnings of Soviet missile attacks during 1979–80 led to alert actions for US strategic forces’, 1 Mar. 2012.

‘should maintain human control and involvement for all actions critical to informing and executing sovereign decisions concerning nuclear weapons employment’.[21] Further, in April and May 2023, two separate bills were launched in the US Congress—one from the Democratic Party and one from the Republican Party—seeking to limit the use of federal funds to launch a nuclear weapon using autonomous weapons systems that lack meaningful human control.[22]

Within China, a 2021 position paper on regulating military applications of AI states that ‘Relevant weapon systems must be under human control, and efforts must be made to ensure human suspension at any time.’[23] While the official document lacks clarity as to which systems are ‘relevant’, some Chinese policy experts and PLA officers have suggested that the ultimate authority for military decision-making for strategic weapon systems should reside with humans.[24]

In the case of the former Soviet Union and Russia, the ‘Perimeter’ nuclear launch control system is believed to enable pre-delegation of authority to ensure nuclear retaliation in response to a hypothetical nuclear decapitation strike by the USA.[25] Nevertheless, Russian officials have stated that the final decision to launch a nuclear strike is to be held by the Russian president, confirming the precedence of the human factor over automated systems.[26] Further, the Oko system malfunction in 1983 indicates that this Soviet early-warning system was not devoid of human intervention, given the critical role of the duty officer.

Improving early warning systems

After the exercise tape insertion and false missile warning in 1979, the US Department of Defense (DOD) constructed a separate facility to train operators so that a tape for training purposes could not again be inserted into the computer running the US early-warning system.[27] Following the Oko early-warning system malfunction in 1983, the Soviet Union launched a new fleet of early-warning satellites into geostationary orbit to provide new angles from which to mitigate sunlight interference and to view US missile fields.[28]

And in 2020, as a further enhancement, Russia modernized the space echelon of its early-warning system by deploying a fourth space vehicle to

[21] US Department of Defense (DOD), ‘2022 Nuclear Posture Review’, in *2022 National Defense Strategy of the United States of America* (DOD: Washington, DC, 27 Oct. 2022), p. 13; and US Department of State, Bureau of Arms Control, Verification and Compliance, ‘Political declaration on responsible military use of artificial intelligence and autonomy’, 16 Feb. 2023.

[22] ‘H. 2894: Block Nuclear Launch by Autonomous Artificial Intelligence Act of 2023’, 118th Congress, 1st Session; and ‘S. 1384: Block Nuclear Launch by Autonomous Artificial Intelligence Act of 2023’, 118th Congress, 1st Session.

[23] Chinese Ministry of Foreign Affairs, ‘Position Paper of the People’s Republic of China on Regulating Military Applications of Artificial Intelligence (AI)’, 14 Dec. 2021.

[24] Yuan Y., Gao D. and Zhang Y., ‘也谈智能化指挥“自主决策”’ [Also talk about intelligent command “autonomous decision-making”], *People’s Liberation Army Daily*, 18 Apr. 2019.

[25] Podvig, P., ‘No gaps in early-warning coverage as three radars to begin combat duty in 2017’, Russian Strategic Nuclear Forces Blog, 23 Dec. 2016.

[26] Legislative Acts of the Russian Federation, ‘Указ Президента Российской Федерации от 2 июня 2020 г. № 355 об Основах государственной политики Российской Федерации в области ядерного сдерживания’ [Presidential decree of 2.06.2020 No. 355 on the Fundamentals of State Policy of the Russian Federation in the field of nuclear deterrence], 2 June 2020.

[27] Forden (note 8).

[28] Forden (note 8).

its unified space detection and targeting system, while digitalizing several parts of the ground segment, including the command and control centres, to enhance data processing and data transmission capabilities.[29] Following reported early-warning assistance from Russia, China's 2022 white paper on its space programme also indicates improved data reception and processing capabilities of the ground system of China's remote-sensing satellites.[30]

Hardening of satellites

In the wake of cyber-related incidents compromising vulnerabilities in satellites between 1998 and 2023, there have been a variety of public and private sector efforts to harden satellites to both jamming and cyberattacks. With a focus on nuclear command and control, starting in 2010, the USA began its launch of an Advanced Extremely High Frequency constellation of communications satellites for high-priority military ground, sea and air assets, which is to be augmented and eventually replaced by the Evolved Strategic Satellite Communications System of nuclear-hardened satellites.[31] Ostensibly, the high frequency and segmentation of these satellite constellations make them more cybersecure.[32] In the case of Russia, Roscosmos more broadly strengthened the cyber defences of its information resources, taking additional measures in July 2022 to secure its Data Processing Center, which receives data from satellites, and its Mission Control Center.[33] And in August 2023 Russia performed tests of digital communications technology to be used for future domestic low-orbit satellite constellations.[34]

The private sector has also contributed to public sector cybersecurity in relation to satellites. The Massachusetts Institute of Technology's Lincoln Laboratory and the Space Cyber-Resiliency group at the Air Force Research Laboratory's (AFRL) Space Vehicles Directorate have developed a spaceflight software platform called Cyber-Hardened Satellite Software (CHSS) for cyber-resiliency of space systems, which eases the burden of defensive cyber operations by constraining bandwidth and utilizing intermittent communication links, combined with cyber-physical safety constraints that enhance predictability.[35] In June 2023 a SpaceX rocket carried a US government Moonlighter satellite to facilitate efforts by five 'white hat', or

[29] 'В России закончили испытания системы предупреждения о ракетном нападении' [Russia has completed tests of a missile attack warning system], RBC, 14 Feb. 2021.

[30] Chinese State Council Information Office, 'China's Space Program: A 2021 Perspective', China National Space Administration, 28 Jan. 2022; 'Russia is helping China build a missile defence system, Putin says', *The Guardian*, 3 Oct. 2019; and Stefanovich, D., 'Russia to help China develop an early warning system', *The Diplomat*, 25 Oct. 2019.

[31] US Space Operations Command, 'Advanced Extremely High Frequency System (AEHF)', Fact sheet, Aug. 2021; 'DRAFT RFP: ESS Space Production Vehicles', Sam.Gov, 6 Oct. 2023; and Erwin, S., 'Space Force planning $8 billion satellite architecture for nuclear command and control', SpaceNews, 25 Oct. 2023.

[32] Erwin, S., 'Future military satcom system puts cybersecurity first', SpaceNews, 19 Nov. 2018.

[33] '"Роскосмос" за полгода отбил кибератак больше, чем за весь прошлый год' ['Roscosmos' repelled more cyberattacks in six months than in the entirety of last year], *Vesti*, 6 Nov. 2022.

[34] 'В России опробована технология цифровой связи посредством низкоорбитальных спутников' [Digital communications technology tested in Russia using low-orbit satellites], *D-Russia.ru*, 17 Aug. 2023.

[35] Skowyra, R. W., Mergendahl, S. A., and Khazan, R., 'Holding the high ground: Defending satellites from cyber attack', *Signal Magazine*, 31 Mar. 2023.

ethical, hacking teams at the Hack-A-Sat (HAS) 4 competition to hijack the satellite and expose its vulnerabilities.[36]

Also using a satellite sandbox, which allows untrusted applications to run in a highly controlled environment, Thales succeeded in April 2023 in meeting the European Space Agency's (ESA) challenge to interfere with the operation of the ESA's OPS-SAT demonstration nanosatellite, by taking over the system that controls the payload's global positioning system, altitude control system and onboard imaging sensor.[37] The 2021 Butian white-hat hacker conference, which is hosted by a subsidiary of Qi An Xin Technology (one of the leading cybersecurity companies in China) also highlighted the vulnerability of space network communications, and Chinese researchers are reportedly building capabilities to 'seize control' of satellites, rendering them useless for data signals or surveillance during wartime.[38]

Protecting ground-based systems and creating hybrid networks

The Viasat KA-SAT cyberattack in 2022 has been transformative in driving efforts to secure ground-based satellite systems and to diversify via hybrid and segregated networks. In January 2023, nearly a year following the attack, the US National Institute of Standards and Technology (NIST) and the MITRE Corporation released a version of the NIST Cybersecurity Framework tailored to the ground-based portion of the space sector.[39] The framework builds on a common approach to cyber defence that includes five major functions: the identification of assets and their cyber-related risks, the development of technologies and procedures to protect those assets, the capability to detect attacks, the infrastructure needed to respond to any incident and the ability to recover from attacks.[40]

Such measures are particularly salient in civilian-operated satellite systems like Viasat and Starlink that combatants have sought to leverage for military operations, and for US companies that contribute to such programmes as the Commercial Solutions for Classified Program requirements for US military satellites.[41] Moreover, the September 2023 US Space Policy Review and Strategy on Protection of Satellites highlights leveraging 'different platforms, different orbits, or systems and capabilities of civil, commercial, or international partners', which includes the US Joint Force employment of both government and commercial satellite communications

[36] Suciu, P., 'Space Force's moonlighter: The hacking sandbox in orbit safeguarding satellite systems', ClearanceJobs, 2 June 2023.

[37] 'Cyberattack on European spacecraft! How "hackers" took control of satellite's imaging sensors & jeopardized its data', *Eurasian Times*, 21 May 2023; Thales, 'Thales seizes control of ESA demonstration satellite in first cybersecurity exercise of its kind', Press release, 25 Apr. 2023; and National Institute of Standards and Technology, Computer Security Resource Centre, 'Sandbox', [n.d.].

[38] Butian, 'Agenda of 2021 Butian White Hat Conference', [n.d.]; and Srivastava, M., Schwartz, F. and Sevastopulo, D., 'China building cyber weapons to hijack enemy satellites, says US leak', *Financial Times*, 21 Apr. 2021.

[39] Lightman, S., Suloway, T. and Brule, J., *Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control*, NIST Interagency Report no. NIST IR 8401 (National Institute of Standards and Technology: Gaithersburg, MD, Dec. 2022).

[40] Lemos, R., 'Space race: Defenses emerge as satellite-focused cyberattacks ramp up', *DarkReading*, 5 Jan. 2023.

[41] US National Security Agency, 'Commercial Solutions for Classified (CSfC)', [n.d.].

systems.[42] Nevertheless, commercial satellites and ground systems face a range of vulnerabilities, including their use of off-the-shelf, open-source technology and software that is subject to screening and cyberattacks. To mitigate these vulnerabilities, Viasat has been working with the US government's AFRL under a seven-year $50.8 million contract to develop concepts for 'hybrid networks' of commercial and government-owned satellites for demonstration purposes.[43]

Legislating cybersecurity of space assets

Informed by such incidents as the ROSAT satellite failures of 1997/98 and the US satellite network infiltration in 2018, the Cybersecurity and Infrastructure Security Agency (CISA) created a Space Systems Critical Infrastructure Working Group in May 2021 by bringing together both government and private-sector stakeholders and tasked the group with offering solutions and developing recommendations to 'effectively manage risk to space based assets and critical functions'.[44] Just five months after the Viasat cyberattack in 2022, a Democratic Party bill for a Satellite Cybersecurity Act was introduced into the US Congress with the aim of strengthening commercial satellite cybersecurity by requiring the CISA to maintain a public repository of resources on the cybersecurity of commercial satellite systems.[45]

China's 2022 white paper on its space programme also highlights an increased focus on strengthening the durability and survivability of its space infrastructure and its information resources, including through the development of a modernized data relay system, and enhanced capacity in 'disaster backup and information protection'. [46] Among these efforts, China has built a new computer system, the OntoCSA4SAT, which reportedly can automatically detect security weaknesses in orbiting satellites and was jointly developed by the National University of Defence Technology in Changsha and the Beijing Aerospace Control Centre.[47]

Although Russia lacks a separate policy on space cybersecurity, it has placed increasing emphasis on the importance of enhancing the security of information and communication technology (ICT) associated with Russian satellites. Released in the same month as the Roscosmos cyber incident, the March 2022 presidential decree on securing critical information infrastructure called for 'the creation . . . of a research and production association specializing in the development, production, technical support and service of trusted software and hardware systems for critical information infrastructure'.[48]

The EU as a body started implementing changes to improve the space industry's cybersecurity posture with the December 2022 update to the EU's

[42] US Department of Defense, 'Space Policy Review and Strategy on Protection of Satellites', Sep. 2023, p. 6.

[43] Erwin (note 1).

[44] Brooks, C., 'The urgency to cyber-secure space assets', *Forbes*, 27 Feb. 2022.

[45] 'S.3511: Satellite Cybersecurity Act', 117th Congress (2021–2022), 21 June 2022.

[46] Chinese State Council Information Office (note 30).

[47] Chen, S., 'Chinese scientists build system "to identify satellite security flaws"', *South China Morning Post*, 9 Apr. 2022; and Tiwari, S., 'China "decodes" an orbiting US satellite; claims expertise in automatically detecting & fixing security flaws in outer space', *Eurasian Times*, 10 Apr. 2022.

[48] Decree of the President of the Russian Federation, 'On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation', 30 Mar. 2022.

Network and Information Security Directive (NIS Directive).[49] EU member states are obliged to transpose the directive into national law by 17 October 2024.[50] Among member states, Germany's Federal Office for Information Security has shaped its National Space Cyber Security Strategy through establishment of a centre of excellence for cybersecurity in spacecraft applications and development of a key and security management system for protected communication channels for the EU's Galileo satellite system.[51] In March 2023 the EU Commission and the EU Agency for the Space Programme announced the first EU Space Strategy for Security and Defence, under which they plan to establish a space-focused Information Sharing and Analysis Centre in 2024. This centre is intended to help private space companies collaborate in cybersecurity, and to launch a multi-orbit satellite constellation called the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS^2), which will rely on quantum cryptography and enhanced cybersecurity through a secure-by-design approach.[52]

Bilateral CBMs

Notifying in advance of missile launch

In the wake of military exercises and false missile alarms due to human error and system malfunction between 1962 and 1983, the former Soviet Union and the USA signed the Agreement on Notifications of ICBM and SLBM Launches during the 1988 Moscow Summit.[53] This document provided for each state to notify the other of any launch of an ICBM or SLBM, no less than 24 hours in advance of the planned launch date, with both the launch area and area of impact. This bilateral agreement was then expanded into the START I Treaty from 1991, which contained an obligation for each state to notify the other of any flight test of an ICBM or SLBM, including those used to launch objects into the upper atmosphere or space, as well as the telemetry broadcast frequencies, modulation types, and choice of encapsulation or encryption to be used. In 2000 the USA and Russia further agreed upon the sharing of early-warning data via a Joint Data Exchange Centre (JDEC) to facilitate launch notifications.[54]

[49] Negreiro, M., 'The NIS2 Directive: A high common level of cybersecurity in the EU', European Parliamentary Research Service, EU Legislation in Progress Briefing PE 689.333, Feb. 2023.

[50] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 Dec. 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), *Official Journal of the European Union*, L333, 27 Dec. 2022.

[51] German Federal Office of Information Security, 'Cyber security for air and space applications', [n.d.].

[52] European Commission, Directorate-General for Defence Industry and Space, 'IRIS^2: The new EU Secure Satellite Constellation', 2023.

[53] Center for Arms Control and Non-Proliferation, 'The Soviet false alarm incident and Able Archer 83' (note 9); Center for Arms Control and Non-Proliferation, 'The Norwegian rocket incident (the Black Brant scare)', Fact sheet, [n.d.]; and Agreement between the United States of America and the Union of Soviet Socialist Republics on Notifications of Launches of Intercontinental Ballistic Missiles and Submarine-Launched Ballistic Missiles (Ballistic Missile Launch Notification Agreement), 31 May 1988.

[54] Memorandum of Agreement between the United States of America and the Russian Federation on the Establishment of a Joint Center for the Exchange of Data from Early Warning Systems and Notifications of Missile Launches, 4 June 2000.

Similarly, in 2010 China and Russia signed a 10-year Agreement on Notification of Launches of Ballistic Missiles and Space Launch Vehicles, which was extended by another 10 years in December 2020, and aimed at 'reducing and ultimately eliminating the risk of nuclear war, in particular as a result of misinterpretation, miscalculation or accident'.[55] By contrast with the Soviet–US agreement, this pre-notification only applied to the launches of ballistic missiles with a range greater than 2000 kilometres directed at each other and notifications did not have to be made publicly.

Engaging in space security exchanges

In July 2020 Russia and the USA held a Space Security Exchange under the framework of the Strategic Security Dialogue to discuss ways to 'enhance communications between the two countries about space-related operational issues' to avoid misunderstanding and inadvertent escalation.[56] The Strategic Security Dialogue was suspended in February 2022 following Russia's invasion of Ukraine. Between China and the USA, there were two major tracks of dialogues on space security: a bilateral Civil Space Dialogue held in Beijing in September 2015, which continued for three rounds; and a bilateral Space Security Exchange held in Washington, DC in May 2016 for only two rounds. The specific details of these dialogues remain undisclosed, and both dialogues were eventually discontinued.[57] In September 2023 the US DOD invited Chinese officials to attend 'working level' meetings to discuss the unclassified summary of the 2023 DOD Cyber Strategy and a range of cyber-related issues.[58] And, in November 2023, China and the USA held official consultations on arms control and non-proliferation, including outer space security issues.[59] However, in both Russia–USA and China–USA cases, it remains unclear as to whether cyber threats to satellite and missile infrastructure were discussed.

Multilateral CBMs

Governing cyberspace and space

While there are a number of United Nations processes relating to cyberspace, the UN group of governmental experts (GGE) on 'advancing responsible state behaviour in cyberspace in the context of international security', and the open-ended working group (OEWG) 'on security of and in the use of information and communications technologies' have not tended to address

[55] Podvig, P., 'Russia and China to exchange launch notifications', Russian Strategic Nuclear Forces Blog, 21 Oct. 2010; and 'China, Russia extend notification agreement for ballistic missile, carrier rocket launches', Xinhua Net, 15 Dec. 2020.

[56] US Department of State, 'The United States and Russia hold space security exchange', Media note, 28 July 2020.

[57] Secure World Foundation, 'The United States, China, and space security: Issues for the Trump administration', Podcast (transcript), 17 Jan. 2017; and MacDonald, B., Freeman, C. and McFarland, A., 'China and strategic instability in space: Pathways to peace in an era of US–China strategic competition', United States Institute of Peace, Special Report No. 515, Feb. 2023.

[58] US Department of Defense, 'US and PRC hold working level meeting on DOD 2023 Cyber Strategy Summary and related cyber issues', Press release, 22 Sep. 2023.

[59] Ministry of Foreign Affairs of the People's Republic of China, 'China and the United States hold consultations on arms control and non-proliferation', Press release, 8 Nov. 2023.

Table 2. Cyber-related missile and satellite confidence-building measures

Originating party or parties in parentheses

Year	Unilateral	Bilateral	Multilateral
1988		Agreement on notifications of ICBM and SLBM launches (USSR, USA)	
1991		START I Treaty (Russia, USA)	
2000		Joint Data Exchange Centre (Russia, USA)	
2004			GGE on cyberspace (China, EU, Russia, USA)[a]
2010	Advanced Extremely High Frequency System (USA)	Agreement on ballistic missiles and space launch notification (China, Russia)	OEWG on reducing space threats (China, EU, Russia, USA)[a]
2015		Civil Space Dialogue (China, USA)	
2016		Space Security Exchange (China, USA)	
2020		Space Security Exchange (Russia, USA)	
2021	Position paper on regulating military applications of AI (China)		OEWG on ICTs (China, EU, Russia, USA)[a]
2022	Nuclear Posture Review (USA) White paper on space programme (China) OntoCSA4Sat (China)[b] Presidential decree on securing critical information infrastructure (Russia) Updated NIS Directive (EU)		
2023	Cyber-Hardened Satellite Software platform (USA)[b] Viasat and AFRL hybrid networks (USA)[a] NIST Cybersecurity Framework for satellite ground segment (USA) Space Strategy for Security and Defence (EU)	Working-level meeting on cyber issues (China, USA)	
2024	Evolved Strategic Satellite Communications System (USA)		

AFRL = Air Force Research Laboratory; AI = artificial intelligence; EU = European Union; GGE = Group of governmental experts; ICBM = intercontinental ballistic missile; ICTs = Information and communication technologies; NIS = Network and Information Security; NIST = National Institute of Standards and Technology; OEWG = Open-ended working group; SLBM = Submarine-launched ballistic missile; USA = United States; USSR = former Soviet Union.

[a] Started in the year.

[b] Reported in the year.

the intersection of cyberspace with space within their various reports.[60] This is in stark contrast to reports from the OEWG on 'reducing space threats through norms, rules and principles of responsible behaviours', which contain multiple references to cyber threats within the space domain.[61]

This acknowledgment of the role of cyber threats also translates into member state contributions to these UN discussions on space. Among these, in 2022 the Chinese official statement made specific reference to the threat

[60] See e.g. United Nations, General Assembly, 'Group of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security', A/76/135, 14 July 2021; and United Nations, General Assembly, 'Developments in the field of information and telecommunications in the context of international security', A/78/265, 1 Aug. 2023.

[61] See e.g. United Nations, General Assembly, 'Reducing space threats through norms, rules and principles of responsible behaviours', A/76/77, 13 July 2021.

of interference with 'launch activities of other countries and disrupting the normal trajectory of outer space objects through electromagnetic interference and cyberattack on the ground, etc.', while the US official statement refers to 'space-based services like navigation satellites and communications satellites being jammed or subject to malicious cyber activities'.[62] Further, the EU's contribution in 2022 advocates for the use of cyberspace, among other domains, as an example in building 'norms of responsible behaviours within legal regimes' within space.[63]

Mapping of cyber-related missile and satellite CBMs

Table 2 shows the above CBMs mapped on a chronological timeline against each category: unilateral, bilateral and multilateral. While acknowledging that this list applies to a narrow set of cyber-related missile and satellite CBMs, it nevertheless indicates a trend towards unilateral statements and documents, and on hardening national systems against cyberattack. By contrast, bilateral and multilateral agreements, exchanges and working groups are limited in number and largely siloed into space, nuclear or cyber domains.

IV. Conclusions

The mapping of cyber-related missile and satellite incidents and CBMs provides a useful means for visualizing current trends, acknowledging that the mapping evolves in relation to the availability of information. From the mapping of cyber-related missile and satellite incidents (table 1) and the mapping of relevant CBMs (table 2) described in this paper, two trends are apparent: (*a*) cyber-related incidents involving missile and satellite infrastructure are increasingly trending towards deliberate targeting; and (*b*) CBMs show a strong tendency towards unilateral statements, documents and efforts to harden systems, rather than the relatively limited bilateral and multilateral measures that are often siloed within space, nuclear or cyber domains. Nevertheless, unilateral CBMs are not without merit, as they enhance reliability and predictability that processes and systems will function as intended. This instils confidence not only domestically, but also internationally that inadvertent human or computer error will not result in escalation or retaliation, particularly when related to missiles or satellites.

As evident from the CBMs discussed above, this finding on unilateral measures applies in a variety of arenas. Among these, there is a marked need to expand upon the application of human control in decision-making and mitigate cases of human error that may trigger panic, escalation and even retaliation. Had the above false missile alarms depended on an autonomous

[62] Li, S., Chinese ambassador, Remarks on topic 2 (Earth-to-space threats), Second substantive session of the open-ended working group on reducing space threats, Geneva, 14 Sep. 2022; and Desautels, E., Acting Deputy Assistant Secretary of State, 'Statement to the open-ended working group on reducing space threats through norms, rules and principles of responsible behavior', Geneva, 9 May 2022.

[63] EU joint contribution on the works of the open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours, 'Fourth part: Recommendations on possible norms, rules and principles of responsible behaviour relating to threats by states to space systems', 2022.

system for retaliation, a number of these cyber incidents could have ended kinetically. Similarly, the cases of human error above point to the importance of independent and multiple points of verification of false alarms and the centrality of strengthened early-warning systems and hardening of satellites. Had hackers succeeded in remotely controlling Roscosmos satellites, as occurred in the case of ROSAT, they could have directed them to collide with other space systems or caused even greater escalation depending on the satellite's intended function. Hardening satellites, protecting ground-based systems and creating hybrid networks are essential measures in protecting space systems when cyberattacks invariably succeed in disrupting their target or in causing spill-over effects. However, while the cooperation of Viasat with the US government's AFRL to develop hybrid networks of commercial and government-owned satellites addresses some of these cybersecurity concerns, this collaboration further blurs the dividing line between civilian and military infrastructure, suggesting the need for greater bilateral and multilateral engagement on this issue.

Ultimately, unilateralism is not necessarily antithetical to confidence building. Unilateral technical means to prevent disruption of satellite systems, false alarms or accidental launch of missiles are stabilizing measures and CBMs that enhance signalling and communication among countries. Further, unilateral release of statements and official documents can also serve as a means of reassurance, and potentially even modelling if others follow suit. Thus, despite the preponderance of unilateral measures above, they still lay the foundation for greater bilateral and multilateral engagement and CBMs on the convergence of interests in defending against cyber threats to missile and space infrastructure. Points of agreement on cyber threats against space assets have already begun to precipitate a degree of multilateral consensus building in the reports and statements surrounding the OEWG on reducing space threats through norms, rules and principles of responsible behaviours. Even points of disagreement, as on the dividing line between civilian and military infrastructure in cyberspace and space, provide important foundations for future bilateral engagement in working-level meetings or strategic stability dialogues. Whether relating to missiles, satellites or other critical infrastructure, mapping cyber incidents and CBMs can assist in visualizing trends to achieve greater predictability and stability in cyberspace.

Abbreviations

AFRL	Air Force Research Laboratory
AI	Artificial intelligence
APT	Advanced persistent threat
CBM	Confidence-building measure
CISA	Cybersecurity and Infrastructure Security Agency
DDoS	Destructive denial-of-service
DOD	Department of Defense
ESA	European Space Agency
EU	European Union
ICBM	Intercontinental ballistic missile
NASA	National Aeronautics and Space Administration
NB65	Network Battalion 65
NIST	National Institute of Standards and Technology
NORAD	North American Aerospace Defense Command
OEWG	Open-ended working group
PLA	People’s Liberation Army
ROSAT	X-ray satellite Röntgensatellit
SLBM	Submarine-launched ballistic missiles

RELATED SIPRI PUBLICATIONS

Cyber Crossover and Its Escalatory Risks for Europe

Dr Lora Saalman, Fei Su and Larisa Saveleva Dovgal
SIPRI Insights on Peace and Security
September 2023

The Role of Space Systems in Nuclear Deterrence

Nivedita Raju and Dr Tytti Erästö
SIPRI Background Paper
September 2023

Naval Incident Management in Europe, East Asia and South East Asia

Dr Ian Anthony, Fei Su and Dr Lora Saalman
SIPRI Insights on Peace and Security
March 2023

Cyber Posture Trends in China, Russia, the United States and the European Union

Dr Lora Saalman, Fei Su and Larisa Saveleva Dovgal
SIPRI Report
December 2022

Explaining the Nuclear Challenges Posed by Emerging and Disruptive Technology: A Primer for European Policymakers and Professionals

Andrew Futter
EUNPDC Paper
March 2021

Cyber-incident Management: Identifying and Dealing with the Risk of Escalation

Johan Turell, Fei Su and Dr Vincent Boulanin
SIPRI Policy Paper
September 2020

RECENT SIPRI PUBLICATIONS

Environmental Politics in Gulf Cooperation Council States: Strengthening the Role of Civil Society
Amal Bourhrous and Emelie Poignant Khafagi
SIPRI Research Policy Paper
November 2023

New Compact, Renewed Impetus: Enhancing the EU's Ability to Act Through its Civilian CSDP
Timo Smit
SIPRI Research Policy Paper
November 2023

The Arctic is Hot: Addressing the Social and Environmental Implications
Emilie Broek
SIPRI Policy Brief
September 2023

Integrating Gender Perspectives into International Humanitarian Law
Nivedita Raju and Laura Bruun
SIPRI Insights on Peace and Security
August 2023

Improving the Prospects for Peace in South Sudan: Spotlight on Measurement
Marie Riquier
SIPRI Policy Report
June 2023

Russia's Military Expenditure During Its War Against Ukraine
Professor Julian Cooper
SIPRI Insights on Peace and Security
June 2023

The Role of Umbrella States in the Global Nuclear Order
Dr Tytti Erästö
SIPRI Insights on Peace and Security
June 2023

Improving the Prospects for Peace in South Sudan: Spotlight on Stabilization
Dr Caroline Delgado
SIPRI Policy Report
May 2023

The World Food Programme's Contribution to Improving the Prospects for Peace in Sri Lanka
Dr Simone Bunse and Dr Vongai Murugani
SIPRI Policy Report
May 2023

STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE
Signalistgatan 9
SE-169 72 Solna, Sweden
Telephone: +46 8 655 97 00
Email: sipri@sipri.org
Internet: www.sipri.org

SIPRI INSIGHTS ON PEACE AND SECURITY NO. 2023/10

MAPPING CYBER-RELATED MISSILE AND SATELLITE INCIDENTS AND CONFIDENCE-BUILDING MEASURES

LORA SAALMAN, LARISA SAVELEVA DOVGAL AND FEI SU

CONTENTS

ABOUT THE AUTHORS

Dr Lora Saalman (United States) is a Senior Researcher within SIPRI's Armament and Disarmament and Conflict, Peace and Security research areas.

Fei Su (China) is a Researcher with SIPRI's China and Asia Security Programme.

Larisa Saveleva Dovgal (Russia) is a Research Assistant with the SIPRI Weapons of Mass Destruction Programme.