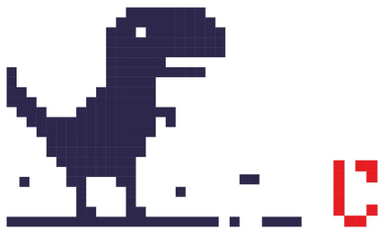
LODZ CYBER HUB
University of Lodz



Twenty-Five Minutes to Midnight

The Accountability Gap

A joint synthesis Submission on behalf of the 2026 Summer School on Internet Governance and International Law (SSIGIL) for the 21st Internet Governance Forum (IGF 2026, Nairobi)

July 2026

Drafted by the SSIGIL 26 Cohort

Facilitators: Jason Bonsall, Dr. Joanna Kulesza

Contributors: Renato Di Stefano, Russell Woruba, Iulia-Alexandra Didu, Dominyka Voiniušytė, Eva-Otilia-Maria Stoicescu, Donatella Casaburo, Kerem Baloglu, Chidimma Achobandu, Kotryna Brežinskaitė, Viktorija Markovaitė, Cioaca Maria Bianca, Turcu Ioana Ivona, Konstantine Japaridze, Solène Rouxel, Cioacă Alexandru Denis, Nițu Luca Ștefan, Georgescu Maia Ștefania, Gheorghe Maria-Veronica, Roberta Carcò, Angela Umano Ciaramella, Sofia Manzhula

Key Finding

The SSIGIL Clock stands at 23:35, twenty-five minutes to midnight.

The law governing state responsibility for harmful cyber operations exists; no venue competent to examine a specific allegation of failure to prevent does. Accusations that cannot be examined are answered politically, and alliance commitments harden around them. This gap, rather than the severity of any single incident, is what brings an uncontainable crisis closer.

1.Introduction

Technology has advanced at a velocity few legal or political institutions have managed to match, and each successive wave, from the earliest packet-switched networks to today's sprawling architecture of cloud infrastructure, artificial intelligence and the Internet of Things, has widened the surface upon which societies now depend and upon which they may equally be struck. Yet this same interconnectedness that has delivered unprecedented prosperity has also conferred unprecedented power upon a comparatively small set of malicious actors, whether states, criminal syndicates or lone opportunists, capable of inflicting damage disproportionate to their size or visibility. It is against this backdrop of accelerating innovation and correspondingly accelerating vulnerability where this question takes on its urgency: how close does each new development bring the international community to a crisis it may no longer be able to contain, and what, if anything, is holding that line?

This proposal traces the collective genesis of the SSIGIL Clock, a multistakeholder assessment of the present cyber landscape and of the body of international law that endeavours to govern it. The exercise was undertaken during SSIGIL 2026 (Summer School on Internet Governance and International Law), convened at the University of Łódź, Poland, which brought together participants from across the legal, technical and policy communities to reckon, collectively, with where the world now stands.

The SSIGIL Clock takes its inspiration from the Doomsday Clock, the enduring symbol devised by the Bulletin of the Atomic Scientists to convey the imminence of nuclear catastrophe in terms a lay audience could grasp at a glance. In place of nuclear peril, the SSIGIL Clock measures the proximity of the international community to a cyber incident capable of metastasising into a global crisis, a scenario Jason Healey terms "Cybergeddon" in his Issue Brief The Five Futures of Cyber Conflict and Cooperation. Over the course of the summer school, participants scrutinised the legal, technical, political and strategic developments shaping cyberspace before jointly determining whether these developments draw the clock's hands nearer to, or further from, midnight.

The Clock's practical value lies in its capacity to render dense legal, technical and policy debate legible to a wider public. Midnight, in this framework, does not signify the inevitability of cyber war; rather, it marks the threshold beyond which failures of international cooperation, weaknesses in cyber governance, or the erosion of critical infrastructure resilience might allow an incident to escalate past the point of effective control. Movement away from midnight, conversely, reflects the opposite: deepening international cooperation, more resilient infrastructure, sharper legal frameworks, and stronger mechanisms for preventing and responding to cyber incidents.

The analysis that follows rests exclusively on the presentations, lectures, workshops and reading materials furnished during SSIGIL 2026, supplemented only where strictly necessary by official legal instruments and publicly available case materials, in order to substantiate the case for moving the dial forward or back. This submission synthesises the principal findings of each day of the programme and assesses how each bears on the overall position of the SSIGIL Clock, weighing the evidence that favours movement away from midnight against the tensions that remain, as yet, unresolved.

2. Daily module summaries: tracing the accountability gap

To fully understand the dimensions of this accountability gap, and the resulting escalation risk, the program was structured as a cumulative progression: rather than treating these legal and geopolitical challenges alone, each day "dismantled" a specific layer of the current cyber landscape, building the necessary foundation for the final consensus.

Day 1: foundations of International Law and Information Warfare.

Main theme: The application of international frameworks, cyber architecture, and weaponized narratives.

This opening module established the conceptual baseline for the program, affirming that international law, including the UN Charter, strictly applies to cyberspace; however, through interactive simulations and policy discussions, the fundamental paradox of cyber governance quickly emerged. Enforcement mechanisms remain critically absent. The module exposed how state actors exploit this lack of universally accepted attribution and dispute resolution mechanism forcing reliance on multistakeholder cooperation, yet leaves the broader system highly vulnerable to destabilization.

Day 2: State responsibility and the power of Due Diligence.

Main theme: shifting accountability from the use of force to state omissions.

Moving beyond the "gridlock" of direct technical attribution, Day 2 focused on the legal duty to prevent. Grounded in the UN Group of Governmental Experts (GGE) framework and the International Law Commission (ILC) Articles on State Responsibility, discussions explored how states owe a duty of due diligence, triggered by knowledge of the risk and understanding of the state's means to prevent internationally wrongful cyber operations originating from their territory. As reflected in the Corfu Channel and Bosnia Genocide precedents, this diligence standard operates below the "use of force" threshold: the framework forces accusations to be tested through formal evidence-sharing rather than escalating through geopolitical "brinkmanship".

Day 3: cybercrime frameworks and fundamental rights.

Main theme: the friction between cross border enforcement and human rights protections.

Examining the Council of Europe's Convention on Cybercrime (Budapest Convention) alongside the new UN Cybercrime Convention (Hanoi Convention), the program analyzed the mechanics of electronic evidence sharing and digital investigations: the critical tension identified lies in oversight. The lack of harmonized regulations creates an accountability gap readily exploited by ransomware networks and criminal proxies and, in order to resolve this, cross-border enforcement must be balanced with strict human rights guardrails under International Covenant on Civil and Political Rights (ICCPR) and European Convention on Human Rights (ECHR) standards. It was highlighted that when states respond to cybercrime with mass surveillance or illusory oversight from DPAs (Data Protection Authorities), they erode geopolitical trust and without rights-respecting

oversight, cross-border cooperation fractures, accelerating conflicts between political blocs.

Day 4: critical infrastructure protection and resilience

Main theme: European regulatory frameworks and the normalization of sub-kinetic attacks.

This day brought the focus to systemic vulnerabilities and the protection of essential services. The module reviewed the European Union's approach as a cyber actor, heavily analyzing the Digital Operational Resilience Act (DORA), the CER directive, and the NIS2 framework. All the discussions underscored an alarming trend: international norms explicitly prohibit damaging essential public services, but the lack of binding global enforcement leaves these vital systems highly vulnerable; state and non-state proxies continually test red lines, exploiting the fact that sub-kinetic attacks on critical infrastructure rarely trigger a conventional military response, normalizing disruption below the threshold of armed conflict.

Day 5: the SSIGIL Clock and IGF 2026 Contribution.

Main theme: consensus building, escalation assessment and policy drafting.

The final day of the school transitioned from theoretical analysis to applied policy drafting; it was dedicated to a student-led exercise aimed at drafting a joint SSIGIL statement on contemporary internet governance challenges for submission to the 21st Internet Governance Forum (IGF) in Nairobi, Kenya. Working groups drafted thematic sections based on the other day's modules, which were then synthesized during the "SSIGIL Clock" capstone exercise (see next pages): the cohort collectively assessed the systemic risk of an alliance-driven cyber escalation, paralleling the 1914 crisis mechanism, and adopted a consensus "time to midnight" in order to reflect the urgency of the accountability gap.

3. Day 5: The SSIGIL Clock and IGF 2026 Contribution: assessing the accountability gap.

SSIGIL 2026 · July 24, 2026 · Facilitators: Jason Bonsall · Dr. Joanna Kulesza

3.1 The deliberation framework: Obligation without a forum.

The conceptual baseline of the SSIGIL cohort's assessment is that cyberspace is not a lawless domain; existing international law, including the United Nations Charter, strictly applies to state conduct online. This principle was affirmed by the UN Group of Governmental Experts in its 2013, 2015 and 2021 reports, and by successive Open-ended Working Groups. That affirmation has proved harder to sustain than to obtain: the GGE process twice ended without a consensus report, and the final report of the 2021–2025 OEWG did not carry forward the reaffirming language that earlier drafts had contained. Agreement that international law applies has not translated into agreement on how. Consequently, states are expected to respect the same fundamental principles online as they do offline, most notably sovereign equality under Article 2(1) of the UN Charter and the prohibition on the threat or use of force under Article 2(4).

However, the cohort identified that acknowledging the applicability of international law does not equate to its effective implementation. There is a long history of describing this landscape as a fatal enforcement failure, as the primary challenge is not the absence of legal rules, but the lack of universally accepted mechanisms for attribution and dispute resolution. To be clear, that is not the position of this report. International law has never possessed centralized enforcement and has functioned regardless.

Two kinds of venue currently exist, and a claim of this nature falls between them. The International Court of Justice and arbitral tribunals possess the competence to determine legal responsibility, but only where the states concerned have consented to their jurisdiction, and no such consent has been extended in any case of this kind. The standing multilateral bodies, namely the GGE process, the successive Open-ended Working Groups, and now the Global Mechanism, operate without any requirement of consent, but their mandate extends to responsible state behavior in general rather than to any specific allegation against a particular state. An allegation that a state has failed to prevent harm originating within its territory is therefore too specific for the bodies capable of hearing it without consent, and too dependent on consent for the bodies competent to decide it. The Global Mechanism, established by General Assembly resolution in November 2025 and

convened for its organizational session in March 2026, represents genuine institutional progress toward continuity of dialogue, but its constitution does not alter this position.

The NotPetya attack of 2017, publicly attributed by several states and causing billions of dollars in global economic damage, exemplifies this gap: the attribution was never examined in any venue capable of testing it, and responsibility was never established anywhere but in the public statements of the attributing states. Similarly, the 2020 SolarWinds compromise demonstrated how disagreements over the legal status of cyber espionage limit the practical application of international law. Notably, the SolarWinds incident was first detected by the private cybersecurity company FireEye, highlighting the reality that much of the technical expertise and infrastructure ownership resides outside government institutions. Without a venue competent to examine the claim, states are left to handle these operations through political or strategic means.

3.2 Competing trajectories: accelerants and restraints

To determine the position of the Clock's hands, the cohort weighed the legal and geopolitical developments that institutionalize prevention against those that exploit the current accountability gap.

The **Restraints** (Institutionalizing Prevention): The strongest legal mechanism to curb state-tolerated cyber aggression before it escalates into overt conflict is the duty of due diligence. The obligation has two sources of differing character. Corfu Channel and the Bosnia Genocide judgment supply the legal foundation. GGE Norm 13(c), by contrast, is a voluntary norm of responsible state behaviour, providing that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. That it commands broad political endorsement while binding no one is itself part of the accountability gap this report describes. The relevant thresholds are set at markedly different levels. Rule 6 of Tallinn Manual 2.0 expresses the due diligence principle in terms of cyber operations producing serious adverse consequences for other states, whereas Rule 69 defines a use of force by reference to scale and effects comparable to a non-cyber operation of that character. The first threshold sits considerably below the second, and the band of conduct falling between them, encompassing ransomware campaigns, severe data theft, and the systemic disruption of essential services, is precisely where the majority of state-tolerated activity occurs. Rule 7 governs compliance, requiring not a guaranteed result but measures that are feasible in the circumstances of the state concerned. This framework forces claims of state omission to be substantiated through documented state practice—formal notification, evidence-sharing, and active cooperation—rather than through geopolitical brinkmanship. The precise scope of that obligation, and the conditions under which a state's failure to act becomes attributable to it, remain contested (Moynihan 2019; Schmid & Erceiş 2023). Alongside this legal doctrine, regional regulatory frameworks provide the clearest evidence of institutionalized prevention. The European Union’s resilience architecture, which includes the Digital Operational Resilience Act (DORA), the NIS2 Directive, the Critical Entities Resilience (CER) Directive, and the 2025 Cyber Solidarity Act, imposes enforceable ICT risk-management, resilience-testing, and incident-reporting obligations across essential sectors. This architecture marks a vital shift from reactive cybersecurity toward anticipatory resilience, supplemented by international cooperation between Computer Emergency Response Teams (CERTs).

The **Accelerants** (Exploiting the Gap): Conversely, significant systemic risks continue to pull the international community toward crisis. In the realm of cross-border cybercrime, the lack of harmonized regulations between the Council of Europe's Budapest Convention and the newly adopted UN Cybercrime Convention (Hanoi Convention) creates an accountability gap. The misuse of technological anonymity allows ransomware ecosystems and criminal proxies to flourish in safe-haven jurisdictions, monetizing this legal void. The cohort noted that when states respond to these threats with mass surveillance or rely on weak, illusory oversight from Data Protection Authorities (DPAs), they erode human rights protections under ICCPR and ECHR standards. This erosion of rights directly deepens geopolitical distrust, fracturing the cross-border cooperation necessary for digital investigations. Furthermore, the gains made by resilience frameworks remain geographically bounded and unevenly transposed by Member States, while the global routing layer, overseen by regional registries like RIPE NCC, still relies almost entirely on the voluntary cooperation of network operators. State institutions are also rendered structurally less capable of

defending themselves due to the private sector's continuous pull on skilled technical and legal talent. Finally, the normalization of sub-kinetic attacks on critical infrastructure creates a paradoxical alliance dynamic: while it restrains escalation within a single incident, it invites a cumulative reading of campaigns that hardens the boundaries between political blocs.

3.3 The “1914 Mechanism”, the deliberation and the final consensus.

The final setting of the SSIGIL Clock required the cohort to identify the pathway by which that threshold is most likely to be crossed. Midnight, as defined above, marks the point beyond which failures of cooperation, weaknesses in governance or the erosion of resilience allow an incident to escalate past effective control. The cohort's judgement was that the mechanism most likely to carry an incident there is not the severity of any single event but the operation of alliance commitments. The cohort named this the "1914 mechanism": a claim that a state has failed to prevent harm which can be neither substantiated nor withdrawn, because no venue of the kind described above is available to examine it and which is therefore answered by pre-positioned collective commitments rather than by evidence (Clark 2012; Dedijer 1966; Miller-Melamed 2022). The position of the hands is determined by the width of the gap between what international law strictly prohibits and the practical machinery available to enforce it. Because no venue is available in which an accusation can be examined, states answer politically and defensive blocs harden. The obligation of due diligence remains the sole corrective, as it demands that claims of omission be substantiated through formal notification, evidence-sharing, and cooperation. The danger is not merely that accusations go untested. In a fragmented cyberspace, joint public attribution comes to operate as much as an act of coalition formation as a determination of responsibility, so that each unexamined claim does double work: it fails to establish anything, and it aligns states against one another regardless (Baram 2026).

When Group 5 convened the open discussion to set the Clock, opening proposals ranged widely, reflecting both pessimistic and hopeful readings of the current landscape. One proposal suggested 23:45, arguing that deep international division, weak regulatory enforcement, and the slow accession of major states to instruments like the Budapest Convention—compounded by the rapid deployment of generative AI—made a significant destabilizing event highly likely within years. Conversely, a second proposal advocated for 23:30, citing growing state investments in education and awareness-building (of which the SSIGIL summer school is a prime example) as evidence of deepening international cooperation. A middle position of 23:40 was also introduced, acknowledging both realities while raising a structural concern: the private sector's continuous pull on skilled technical and legal talent leaves state institutions less equipped to defend themselves.

While the majority of the working groups initially leaned toward 23:30 on the grounds of cautious optimism, a critical counter-argument held that alliance dynamics are already primed to the point that the interval between an untested accusation and a collective answer must be measured in minutes. The cohort acknowledged that adversaries—whether in cybercrime or infrastructure interference—now operate through sustained campaigns rather than discrete incidents. An effects-based threshold keyed to single events is blind to these campaigns; only due diligence, triggered by the knowledge of risk and assessed over time, runs on the adversary's clock. Furthermore, while the European Union’s resilience architecture represents genuine progress, it buys time at the level of consequence, not intent, and remains strictly regional while the threatened infrastructure is global.

The definitive shift to the final consensus time was prompted when the floor opened to the wider room of participants, bringing the cross-cutting risk of manipulated information (misinformation, disinformation, and malinformation) to the center of the debate, referencing its threat to core functions of a state such as election, public health, and insitutional trust. This sparked a profound discussion on how international law does not recognize a general prohibition on the dissemination of false information. However, It is important to include that the category of foreign information manipulation and interference (FIMI), in international law, remains a classification of that policy rather than a legal one and there is no obligation that binds states to this policy. Therefore, an

argument in favor of restricting this flow of information would need to be based in human right instruments rather than any dedicated prohibition. Nevertheless, Opinions fractured: some argued that neither governments nor private platforms should possess the authority to arbitrate truth. Article 19(2) and (3) of the ICCPR supports this view by protecting the freedom of expression and lets the state control its restriction under national law and for a specific purpose. Others countered that free expression is not absolute, and that the same legal reasoning justifying state intervention against hate speech extends to harmful online disinformation. This second view is grounded in Article 20(2) of the ICCPR, which requires states to prohibit advocacy of hatred based on nationality, race or religion where it incited discrimination, hostility or violence. This second view centers speech around the harm is causes rather than accuracy of its content presenting a conflict to the first view. Yet still a third faction maintained that widening public access to accurate information could mitigate the harm without requiring the direct suppression of speech. This third take avoids the threshold mentioned in Article 19(3) altogether by supplementing the information environment rather than restrict it.

Despite these differing approaches, the cohort unanimously recognized the systemic impact of manipulated information. Generative AI systems are compressing the cost of producing state-sponsored propaganda faster than global governance can adapt. The ultimate harm of this manipulation is the deliberate erosion of the shared factual ground upon which any claim of state omission must be tested. Without a verified factual baseline, attribution ceases to be a finding of fact and becomes merely an act of political alignment.

Recognizing that these risks are substantial, shared across all states, and unusually resistant to conventional regulation, the cohort agreed to advance the time by five minutes from the most optimistic estimates. The SSIGIL Clock therefore stands at 23:35 — twenty-five minutes to midnight. The ultimate conclusion of the assembly was that moving the hands back does not require drafting a new treaty. What is absent is not jurisdiction but competence: a standing body whose mandate extends to examining a specific allegation that a state failed to prevent harm. Mandates are conferred by the states that constitute such bodies, and can be extended by them.

4. Policy questions for the Forum.

The Clock records where the cohort believes the international community now stands. It does not settle the questions that put it there, and the case for bringing the instrument to Nairobi rests on the fact that those questions remain genuinely open — the cohort divided on each of them over the course of the week. Three are put forward for discussion at IGF 2026, in the order the argument runs: what is changing in the capability of actors, what that change does to the practice of attribution, and what might be done about it without waiting for a new treaty.

One. As AI systems reduce the expertise required to discover and exploit vulnerabilities in widely used software, the population of actors capable of causing serious harm may grow faster than any state's capacity to supervise conduct on its own territory. Are the mechanisms currently relied upon to prevent that harm — state due diligence obligations, cybercrime cooperation frameworks and coordinated vulnerability disclosure — capable of absorbing that shift, and what would genuine preparedness require?

The week's third and fourth modules both described adversaries who are not states: ransomware ecosystems operating as enterprises across jurisdictions, and proxies testing infrastructure red lines beneath the threshold that would draw a conventional response. Both analyses assumed a population of capable actors bounded by the scarcity of technical skill. That assumption is the one now in question, and every framework surveyed during the week was built while it still held.

Two. If technical sophistication is no longer evidence of state sponsorship, how are states to distinguish conduct they have tolerated from conduct they have directed? Does that growing ambiguity make untested public attribution, and the alliance dynamics that follow from it, more likely rather than less?

This is where the first question meets the accountability gap. Sophistication has served as an informal evidentiary shortcut: operations of a certain complexity were taken to imply state resources, and therefore state involvement. If that inference weakens, the distinction between an act a state directed and an act it merely failed to prevent becomes harder to draw at precisely the moment when drawing it wrongly carries the gravest consequences. The 1914 parallel the cohort adopted turns on this exact difficulty — a claim of failure to prevent that could be neither substantiated nor withdrawn.

Three. Courts can decide such claims but only by consent, which is never given; the standing multilateral bodies can convene discussion of responsible behaviour in general but cannot take up a specific allegation that a state failed to prevent harm originating from its territory. What arrangements short of a new treaty would allow such claims to be examined before they are answered politically?

The cohort's judgement is that the necessary law already exists. Corfu Channel and GGE Norm 13(c) establish an obligation of prevention, and Tallinn Manual 2.0 restates it at Rule 6 in terms that attach well below the threshold its Rule 69 sets for a use of force. What is absent is any venue in which a state can be asked to answer for it. The question is therefore institutional rather than doctrinal, and the cohort puts it to the Forum in that form deliberately: what would have to be built, and by whom, for the hands to move back.

5. The instrument beyond Łódź

The Clock represents a collective synthesis rather than a static truth, reflecting the deliberations of a specific cohort within a finite timeframe. Its utility is found not in the numeric output, but in the analytical rigor the methodology demands: to move the hands, one must scrutinize shifting technical capabilities, balance them against institutional anchors, and justify that assessment against competing interpretations of the same landscape. This intellectual framework is designed to be mobile; the exhaustive reasoning in Section 3 is provided specifically to invite scrutiny, contestation, and refinement by the broader community.

Consequently, 23:35 is submitted as an initial baseline rather than a final verdict. At IGF 2026, the methodology is handed to the Forum at large, where participants are encouraged to interrogate the underlying logic, introduce independent evidence, and collectively determine the setting in the room. Should the Forum's consensus diverge from this initial assessment, the substantive value lies in the documented reasons for that shift. Where consensus proves elusive, the very nature of that fragmentation is recorded as a finding in its own right, as disagreement over the imminence of crisis is itself a vital indicator of the state of global cyber governance.

The cohort advocates for the Clock to be set annually at each subsequent Forum. If a single setting captures a snapshot, a sequence reveals a trajectory, allowing the international community to measure whether specific regulatory restraints or technical accelerants are delivering on their promises. Much like the Doomsday Clock, the instrument's significance grows through the accumulation of successive readings. An assessment owned and updated by the multistakeholder community would provide internet governance with a critical, missing component: a longitudinal, publicly reasoned record of the world's proximity to a threshold it may not be able to contain.

Comparative Cybersecurity Policy Heat Map

This is an analytical heat map, rather than an official EU classification based on the discussions from SSIGIL summer school. The existing cyber policies, directives and legislative instruments have been assessed across the respective risk and policy domains.

Legend:

- ●●● = primary/strong coverage
- ●● = significant coverage
- ● = limited/indirect coverage
- — = largely outside core purpose

Risk / policy domain	NIS1 (repealed 2024)	NIS2	CER	DORA	CRA	Cyber Solidarity
Organisational cyber risk	●●	●●●	●	●●●	●	●
Network/system security	●●●	●●●	●	●●●	●●	●●
Board/governance accountability	●	●●●	●●	●●●	●●	●
Supply-chain cyber risk	●	●●●	●●	●●●	●●●	●●
Cloud/ICT provider dependency	●	●●●	●	●●●	●	●●
Physical infrastructure risk	—	●	●●●	●	—	●
Natural hazards	—	●	●●●	●●	—	●
Business continuity	●●	●●●	●●●	●●●	●	●●
Financial systemic ICT risk	●	●●	●	●●●	●	●●
Product cybersecurity	—	●	—	●	●●●	—
Security-by-design	●	●●	—	●●	●●●	—
Vulnerability lifecycle	●	●●●	—	●●	●●●	●●
Incident reporting	●●	●●●	●●●	●●●	●●●	●●
Threat intelligence	●●	●●●	●	●●	●	●●●

Cross-border crisis response	●●	●●●	●●	●●	—	●●●
Shared EU response resources	—	●	●	—	—	●●●
Large-scale cyber crisis	●	●●●	●●	●●	—	●●●
Post-incident EU learning	●	●●	●	●●	●	●●●

Works Cited

Treaties and international instruments

Charter of the United Nations, 26 June 1945, 1 UNTS XVI.

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), 4 November 1950, ETS No. 5.

International Covenant on Civil and Political Rights, 16 December 1966, 999 UNTS 171.

Council of Europe, Convention on Cybercrime (Budapest Convention), 23 November 2001, ETS No. 185.

United Nations Convention against Cybercrime (Hanoi Convention), adopted by UN General Assembly Resolution 79/243, 24 December 2024.

Cases

Corfu Channel Case (United Kingdom v. Albania), Merits, Judgment of 9 April 1949, ICJ Reports 1949, p. 4.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment of 26 February 2007, ICJ Reports 2007, p. 43.

United Nations documents

International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, 2001, annexed to UN General Assembly Resolution 56/83.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013.

Report of the Group of Governmental Experts …, UN Doc. A/70/174, 22 July 2015.

Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135, 14 July 2021.

Final Substantive Report of the Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security, UN Doc. A/75/816, 18 March 2021.

European Union legislation

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS1), OJ L 194/1. repealed with effect from 18 October 2024 by Directive (EU) 2022/2555

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), OJ L 333/1.

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2), OJ L 333/80.

Directive (EU) 2022/2557 on the resilience of critical entities (CER), OJ L 333/164.

Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), OJ L, 2024/2847.

Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), OJ L, 2025/38, 15.1.2025.

Books, articles and reports

Clark, C. (2012). *The Sleepwalkers: How Europe Went to War in 1914*. London: Allen Lane.

Dedijer, V. (1966). *The Road to Sarajevo*. New York: Simon and Schuster.

Healey, J. (2011). *The Five Futures of Cyber Conflict and Cooperation*. Atlantic Council Issue Brief, December 2011. Also published in *Georgetown Journal of International Affairs*, Special Issue: International Engagement on Cyber (2011), 110–117.

Miller-Melamed, P. (2022). *Misfire: The Sarajevo Assassination and the Winding Road to World War I*. New York: Oxford University Press.

Moynihan, H. (2019). *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention*. London: Chatham House Research Paper.

Schmid, E., & Erceiş, A. Ö. (2023). The attribution of omissions: Due diligence in cyberspace and state responsibility. *Swiss Review of International and European Law*, 33(4), 577–596.

Schmitt, M. N. (ed.) (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. Prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence.

Baram, G. (2026). Re-ordering accountability: The significance of joint public attribution in a fragmented cyberspace. *Contemporary Security Policy*, advance online publication. https://doi.org/10.1080/13523260.2026.2662220