Research Paper

International Law Programme

January 2026

Securing justice for cyber-enabled international crimes

Legal foundations and practical routes to prosecution

Elizabeth Wilmshurst, Harriet Moynihan and Tsvetelina van Benthem

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies to build a secure, sustainable, prosperous and just world.

Contents

Summary

- Harmful cyber operations are growing in pace, scale and impact. Cyber operations targeting critical infrastructure have increased significantly in recent years. The number of cyber actors is also on the rise, with generative AI aiding criminals in carrying out their operations.
- Many states now have laws that criminalize cyber activity such as online fraud and hacking. But cyber means can also be used to facilitate or commit the *international* crimes of genocide, crimes against humanity, war crimes and aggression. There is an urgent need to improve the prospects for prosecution of such crimes when committed or facilitated by cyber means.
- A harmful cyber operation may constitute both a cybercrime and a cyber-enabled international crime – for example, a war crime facilitated by cyber means may include illegal hacking. Attempts to hold those responsible for cyber-enabled international crimes accountable are likely to use some of the routes, tactics and actors involved in prosecuting cybercrime. At the same time, prosecutions for the distinct wrong of cyber-enabled international crimes also require reliance on the apparatus of international criminal justice.
- International criminal law is technology-neutral – an international crime is a crime whether committed using a gun or a computer. States and the International Criminal Court (ICC) can and should prosecute individuals for their involvement in cyber-enabled international crimes. In December 2025, the ICC Office of the Prosecutor (OTP) published its 'Policy on Cyber-Enabled Crimes under the Rome Statute'. This policy paper makes clear the OTP's intention to investigate and prosecute cyber-enabled crimes under the Rome Statute on an equal basis with such crimes committed by more traditional means.
- Our research paper elaborates on the OTP policy paper and discusses ways for states to prosecute cyber-enabled international crimes, whether individually or jointly. In doing so, it highlights for all stakeholders the relevance of international criminal law to cyber activity. Our paper is also intended to be of use to states as they prepare or update future national position statements on the application of international law to cyberspace in the context of discussions at the UN on a Framework for Responsible State Behaviour in Cyberspace.
- Our paper explores key questions on responsibility for cyber-enabled international crimes, including:
  - In what circumstances are individuals causing harm by cyber means guilty of an international crime?
  - Are the providers of cyber infrastructure complicit when that infrastructure is used by others to commit international crimes?

  - How do we determine complicity?
  - How can we prove who is criminally responsible when all cyber activity seems shrouded in secrecy?
  - Are investigators, prosecutors and judges ready for these kinds of cases, and, if not, what more needs to be done?
- In clarifying how international criminal law applies in the cyber context, this paper responds to the need for guidance for cyber actors of all kinds – including states, technology companies, hacker groups and individuals – regarding the constraints imposed on their activities by international criminal law and the possibilities of prosecution. The paper also examines the challenges and opportunities of investigating and prosecuting cyber-enabled international crimes in practice, and suggests ways in which various actors can help to improve the prospects for successful prosecutions in future.
- The paper concludes with recommendations for strengthening accountability for cyber-enabled crimes, aimed at all relevant actors. These recommendations include:
  - Strengthened cooperation between actors at various levels – including states; the OTP; international organizations such as Eurojust, Europol and Interpol; private companies such as social media platforms and cyber intelligence services; and civil society.
  - Ensuring that states have the necessary domestic law to prosecute cyber-enabled international crimes, and the ability to cooperate with others where they do not have the necessary resources themselves. Prosecution authorities should enhance their cyber expertise and their networks with the recruitment of cyber intelligence experts. States should ensure they are sufficiently cooperating with the ICC.
  - Adequate in-house cyber expertise within the OTP to enable it to bring successful prosecutions. The OTP should also seek to enhance its cooperation with investigators and prosecutors in states and international organizations, particularly the EU, and with private entities.
  - Robust procedures within technology companies to identify and mitigate the risks of participation in harmful cyber activity. Companies should facilitate requests for evidence from law enforcement agencies and the OTP.
  - The establishment by civil society or academia of a database of ongoing domestic and international prosecutions of cyber-enabled crimes as a repository of know-how for all actors to draw on. Civil society organizations can also help build trust and understanding between different stakeholders and facilitate discussion on how to strengthen accountability for cyber-enabled international crimes.
  - Prioritizing training for investigators, prosecutors and judges. States and international tribunals also need to ensure that they have facilities to store, preserve, authenticate and analyse the significant amount of evidence involved in the prosecution of cyber-enabled international crimes.

01 Introduction

More attention is needed on how international criminal law applies to cyber operations. This Chatham House research paper follows a new policy issued by the Office of the Prosecutor of the International Criminal Court. Both seek to fill that gap.

As society's dependence on information and communication technologies (ICTs) grows, so does its vulnerability to attack. Recent examples include the Russian army using cyber capabilities to shut down power grids in Ukraine,[1] state-sponsored hackers infiltrating water supplies,[2] and the hacking of nuclear sites.[3]

There is a risk of impunity for those using the most harmful forms of cyber activity. States have consistently affirmed that existing international law, including the UN Charter, applies to the cyber activities of states.[4] But, until recently, little attention has been paid to whether individuals who inflict serious harm by cyber means can be held responsible under international criminal law and, if so, how.

Many national laws already cover 'cybercrimes' such as online fraud, theft or hacking. But there are some circumstances in which the nature and severity of cyber operations place them in an additional category – that of an international

---

1 Pearson, J. (2023), 'Russian spies behind cyber attack on Ukraine power grid in 2022 – researchers', Reuters, 9 November 2023, https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09.
2 O'Flaherty, K. (2024), 'AI Autopsy: American Water Cyber Attack', Assured Intelligence, 22 October 2024, https://assured.co.uk/2024/ai-autopsy-american-water-cyber-attack.
3 Isaac, A. and Lawson, A. (2023), 'Sellafield nuclear site hacked by groups linked to Russia', *Guardian*, 4 December 2023, https://www.theguardian.com/business/2023/dec/04/sellafield-nuclear-site-hacked-groups-russia-china.
4 See, for example, UN General Assembly (2025), *Open-ended working group on security of and in the use of information and communications technologies 2021-2025, Draft Final Report*, 11 July 2025, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Letter_from_OEWG_Chair_10_July_2025.pdf; African Union Peace and Security Council (2024), *Communiqué of the 1196th meeting of the Peace and Security Council held on 29 January 2024 considering the Draft Common African Union Position on the Application of International Law to the Use of Information and Communication Technologies and Cyberspace*, updated 6 February 2024, https://www.peaceau.org/en/article/communique-of-the-1196th-meeting-of-the-peace-and-security-council-held-on-29-january-2024-considering-the-draft-common-african-position-on-the-application-of-international-law-to-the-use-of-information-and-communication-technologies-in-the-cyberspace; Council of the European Union (2024), *Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace*, 18 November 2024, https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf.

crime. It is notable that, of the states that have published position statements so far on the application of international law to cyberspace (over 100, factoring in regional position statements), only one – Austria – has so far referred to international criminal law.[5]

While it has become evident that no new law is required to capture the core international crimes when carried out by cyber means, further attention is needed as to the way in which the existing law applies to the circumstances of cyber operations. There is also a need to confront the particular challenges that arise when the perpetrators of cyber-enabled international crimes are brought to justice. While the difficulties should not be underestimated, the existence of an effective framework for investigation and prosecution of such crimes may help to prevent them.

About this paper

In 2024 and 2025, Chatham House's International Law Programme hosted expert roundtable discussions, held under the Chatham House Rule,[6] on the strengthening of accountability for cyber-enabled international crimes. These discussions were attended by government legal advisers and prosecution authorities, officers from the ICC, representatives from technology companies, and leading academic experts in the fields of international humanitarian law and international criminal law. The International Law Programme also conducted desk research, literature reviews and interviews with experts. This paper draws on insights from each of these sources.[7]

The objectives of the paper are:

- To clarify which cyber activities come within the range of international criminal law (Chapter 2);
- To consider the legal framework for securing justice effectively (Chapter 3);
- To discuss the opportunities and challenges involved in pursuing accountability for committing international crimes; and to consider how the challenges might be addressed, including how to promote effective partnerships between courts, states and the private sector (Chapter 4); and
- To make recommendations on how to strengthen avenues for accountability in this area (Chapter 5).

---

5 Government of Austria via Cyber Law Toolkit (2024), 'National position of Austria: Individual criminal responsibility under international law', https://cyberlaw.ccdcoe.org/wiki/National_position_of_Austria_(2024)#Individual_criminal_responsibility_under_international_law.
6 'When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.' See Chatham House (undated), 'Chatham House Rule', https://www.chathamhouse.org/about-us/chatham-house-rule.
7 The paper has also benefited from a report by the Council of Advisers on the application of the Rome Statute to cyberwarfare and a draft chapter of the Tallinn Manual 3.0 on the International Law Applicable to Cyber Operations (forthcoming). See Council of Advisers (2021), *The Council Of Advisers' Report On The Application Of The Rome Statute Of The International Criminal Court To Cyberwarfare*, report, August 2021, https://crimeofaggression.info/wp-content/uploads/GIPA_The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf.

In this paper, the term 'cyber' refers not just to traditional cyber technologies (such as those used in ransomware or hacking operations), but also to digital technologies more broadly (including social media networks and the internet). The term 'cyber-enabled international crimes' refers to genocide, crimes against humanity, war crimes and aggression committed or facilitated by cyber means. 'Cybercrimes', on the other hand, are defined in international treaties as including online fraud, theft or hacking.[8] They do not fall in the category of core international crimes as such, though it is possible for a cyber operation to constitute both a cybercrime and an international crime.

This research paper brings the OTP's policy[9] to a wider audience, expands on certain issues arising from that policy and proposes solutions to some of the challenges in the field. Our paper also widens the discussion to explore the role of *national* courts, as it should ordinarily fall on them to prosecute, where possible, cyber-enabled international crimes. Though its main object is to explain the ICC's prosecution policy, the OTP paper is likely in addition to be a useful guide to all countries on their own investigation and prosecution of international crimes.

8 See, for example, The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols ('Budapest Convention'), open for signature 23 November 2001, entered into force 1 July 2004, https://www.coe.int/en/web/cybercrime/the-budapest-convention, e.g. arts 1 and 8; United Nations Convention against Cybercrime, Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, General Assembly, 24 December 2024 ('UN Convention against Cybercrime'), UN Doc A/79/460, https://docs.un.org/en/A/79/460, arts 7 and 13.
9 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, December 2025, https://www.icc-cpi.int/news/policy-cyber-enabled-crimes-under-rome-statute.

02 Applying international criminal law to harmful cyber operations

Harmful cyber operations can enable the commission of international crimes or, in some circumstances, can themselves constitute international crimes.

The Statute of the ICC defines four kinds of core international crimes – genocide, crimes against humanity, war crimes and aggression. Although these are sometimes referred to as crimes under the ICC Statute (also known as 'the Rome Statute'), it was not that treaty that originally created the crimes. Generally speaking, these crimes also exist independently of the ICC, under pre-existing rules of international law – whether under treaty law or under customary international law. Some or all of them have been incorporated into the legislation of many states,[10] and can therefore be prosecuted in those states whether they are party to the ICC or not.

10 See Chapter 3 of this paper.

International criminal law concerns the criminal responsibility of *individuals*. If harmful cyber operations are attributable to a *state*, responsibility may arise at two levels: i) the state may be held responsible under the general rules of international law; and ii) individual state agents may also be prosecuted under the branch of international law that is international criminal law. Prosecutions under international criminal law may also be possible, of course, if there is no state involved and the individual is acting under their own authority or with a non-state group.[11] It should be noted that crimes can only be committed by natural persons (at least under the Rome Statute), thus excluding corporations and inanimate artefacts, such as AI applications. AI can, however, be used as a tool by individuals – including developers, programmers, operators and commanders.

While international criminal law evolved at a time before most of the current forms of ICTs were in existence, there is no reason why it should not be applicable to them – as it is applicable to *all* means of committing crimes.

The law is technology-neutral. While international criminal law evolved at a time before most of the current forms of ICTs were in existence, there is no reason why it should not be applicable to them – as it is applicable to *all* means of committing crimes. International crimes can be committed by cyber means alone – for example, by hacking into a nuclear power station with the intention of causing thousands of deaths. However, cyber operations are more typically used as part of a wider set of acts. An example from the context of an armed conflict could be where cyber operations disable civilian infrastructure as part of the overall campaign.

There are some differences between the definitions of crimes in the ICC Statute and those included in other treaties, custom and in national law. But for clarity, the wording of the ICC Statute is used in this paper. Our paper is not intended to be a comprehensive account of the four core international crimes. It focuses simply on some aspects relevant to the commission of the four crimes by cyber means.

As with the case studies given later in the paper, the examples given below in text boxes are intended to be credible illustrations of acts to which international criminal law can be applied. Though hypothetical, some of these examples already reflect reality.

11 The crime of aggression entails different considerations.

2.1 Genocide

Example

In the course of a campaign to wipe out members of a minority group, government operators are ordered to launch a cyber attack against the computer network of the health system in the part of the country where the group resides, directly causing injuries and deaths.

Genocide denies the right of certain human groups to exist. The aim of a *genocidaire* to wipe out a protected group, or part of one, is what sets this crime apart from other international crimes. The standard definition of genocide is to be found in the Genocide Convention of 1948, which is repeated in the Rome Statute and in national legislation.[12]

Genocide consists of 'any of the following acts committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such:

1. Killing members of the group;
2. Causing serious bodily or mental harm to members of the group;
3. Deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part;
4. Imposing measures intended to prevent births within the group;
5. Forcibly transferring children of the group to another group.'[13]

All of the listed acts could be committed by cyber means.[14] For example, a cyber operation might interfere with the working of a dam, with the aim of flooding the villages of a protected group. That act could qualify as genocide by the killing of members of the group. Or a cyber operation affecting an electricity network, with severe impacts on electricity and the supply of water, may inflict on a group conditions of life calculated to bring about its physical destruction. Both these examples illustrate that they are likely to be undertaken not alone but in conjunction with other, non-cyber acts.

12 Rome Statute of the International Criminal Court, UNTS 2187, 17 July 1998 ('Rome Statute'), art. 6. States that have adopted this definition include Australia, Brazil, the Democratic Republic of the Congo, France, Germany, South Africa and the UK. A few countries – including Bangladesh, Colombia, Costa Rica, Ethiopia, Lithuania and Poland – have extended the definition of genocide in their national law to include destruction of other groups, such as political groups. See Nersessian, D. (2010), *Genocide and Political Groups*, Oxford University Press, ch. 5.
13 Convention on the Prevention and Punishment of the Crime of Genocide, UNTS 78, 9 December 1948 ('Genocide Convention'), art. II.
14 See Council of Advisers (2021), *The Council Of Advisers' Report On The Application Of The Rome Statute Of The International Criminal Court To Cyberwarfare*, pp. 77–85.

For genocide to be successfully prosecuted, it is not enough to show that one of the listed acts has been committed, with the intent to commit that act. There must also be a genocidal intent. The crime is committed only if the perpetrator means to commit the act in question, and in addition has an intention to 'destroy' the protected group. The reference is specifically to physical or biological destruction, not simply to social assimilation into other groups, for example. And the members of the protected group must be targeted *because of* their membership of the group. It is not, however, necessary to show a large number of deaths.[15]

Direct evidence of genocidal intent may be difficult to find. It is possible, however, to infer intent from circumstantial evidence.[16] Cyber activities may be particularly important in grounding the relevant inference. A campaign on social media, for example, against the protected group might assist in proving intent.

Incitement to genocide

'Direct and public incitement' to commit genocide is specifically prohibited in the Genocide Convention. It is an offence, whether or not genocide is actually committed as a result of the incitement. Such a crime can easily be committed by cyber means – for example, by posting statements on social media platforms. Modalities of online expression such as liking, sharing or hosting content posted by others may also be relevant in this context. The status of the person creating or amplifying the speech act and the reach of their expression are relevant to the assessment of incitement. But 'mere' hate speech that does not call for genocidal acts is not enough. There must also be genocidal intent.[17]

A case before the International Criminal Tribunal for Rwanda (ICTR) is illustrative. This concerned the use of radio broadcasts in 1994, which were important in Rwanda as a source of information as well as a focus of social life. At a time when the genocide against the Tutsis was beginning, Ferdinand Nahimana was on the steering committee of a national radio station, Radio Télévision Libre des Milles Collines (RTLM), and was one of those responsible for the station's programming. Broadcasts via RTLM were used to promote hatred of the Tutsis and to call for their extermination. Nahimana was found guilty of direct and public incitement to commit genocide.[18]

---

15 *Krstić* (ICTY Appeal Chamber Judgment) IT-98-33-A (19 April 2004), para 12.
16 See Report of the Detailed Findings of the Independent Fact-Finding Mission on Myanmar', A/HRC/39/CRP.2 (17 September 2018), paras 1415–26, and the ICTY caselaw cited there.
17 For prosecutions in the ICC at least, the occasional posting on social media may not reach the threshold of 'gravity' that is not only required as a criterion of admissibility, but which also may be taken into account by the prosecutor in the exercise of discretion as to which cases to bring before the court.
18 *Nahimana et al*, Trial Chamber Judgment, ICTR-99-52-T (3 December 2003) and Appeals Chamber Judgment, ICTR-99-52-A (28 November 2007).

2.2 Crimes against humanity

Examples

A rebel group is undertaking a process of widespread destruction to force the government to accede to their demands. Some of their members mount computer network attacks which disable air traffic control systems, resulting in aircraft crashes and numerous deaths.

In another state, government officials begin a campaign against women for so-called religious reasons, systematically removing their access to civil rights, authorizing violent means of implementing discriminatory legislation and undertaking mass surveillance to ensure complete enforcement of the law, causing alarm and terror.

Crimes against humanity can be loosely regarded as the multiple commission of atrocities or rights violations. A crime is committed if one or more of a list of acts is 'part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack'.[19] Crimes against humanity can be committed in a time of peace, as well as during armed conflict, and the context of a 'widespread or systematic attack' is not confined to military attacks. 'Attack' here means 'a course of conduct involving the multiple commission' of the acts listed, 'as part of a State or organisational policy'.[20]

The list of individual acts encompassed within the definition of crimes against humanity includes murder, enslavement, deportation, imprisonment, torture, rape and other serious forms of sexual violence, and persecution of a group.

An online act that corresponds to one of the acts mentioned will amount to a crime against humanity if it is part of a 'widespread or systematic attack'.

An online act that corresponds to one of the acts mentioned above will amount to a crime against humanity if it is part of a 'widespread or systematic attack'. While it is possible to imagine the whole of an 'attack' being carried out by cyber means, it is perhaps more likely that the cyber conduct will be committed alongside other physical acts. As in the examples in the box above, a single cyber operation could thus meet the required threshold, if carried out as part of a wider attack.

Some in the list of acts can be committed either wholly or partially by cyber means (e.g. murder or persecution): for example, using cyber operations to cause the bursting of dams with fatal effects, or disabling power systems or medical infrastructure causing injuries and deaths. And social media and digital surveillance might be used to assist a campaign of persecuting an ethnic minority. It is difficult

19 Rome Statute, art. 7(1).
20 Rome Statute, art. 7(2)(a). While this is a requirement in the Rome Statute, it is less clear that it is required under customary international law.

to imagine that other acts on the list can be committed by cyber means alone (e.g. imprisonment), although cyber means could be used to facilitate the crime.

Unlike in the crime of genocide, there is generally no special requirement regarding intent for crimes against humanity. But it is necessary for the perpetrator to know both that their conduct forms part of the 'attack' and to have the necessary intention to commit the act itself.[21]

2.3 War crimes

Examples

In an ongoing armed conflict between two states, one state's agents introduce malware into the computer systems of the opposing state, rendering much of them inoperable, deleting data and causing widespread damage to civilian infrastructure – including hospitals and emergency services.

In a civil war, a fighter photographs captured prisoners in degrading and humiliating positions and posts the images on social media.

International humanitarian law (or the law of armed conflict) imposes obligations on parties to armed conflict in relation to the conduct of hostilities and the protection of civilians, the sick and wounded and prisoners of war. This body of law aims to place limits on the destruction and suffering caused by armed conflict. Violations of many, but not all, of its provisions gives rise to individual criminal responsibility for war crimes. The definitions of war crimes are thus based on the underlying provisions of international humanitarian law and need to be interpreted in accordance with that body of law. Soldiers must know when they are acting in accordance with the laws of war, and thus international criminal law, or not.

It is only when there is an armed conflict – whether international or non-international – that responsibility for war crimes may arise. And the relevant conduct must take place in the context of, and be associated with, the armed conflict.[22] Although it is theoretically possible that an armed conflict can be *begun* by cyber operations,[23] it is more likely that any war crimes committed by cyber means will be taking place as part of an ongoing armed conflict.

The Geneva Conventions and Protocol I require states to criminalize so-called 'grave breaches' of the laws of war committed in international armed conflict.[24] In addition,

---

21 For discussion of *unintended* harms, see p. 19.
22 See, for example, the ICC Elements of Crimes, art 8, chapeau.
23 This is certainly the view of the OTP policy paper. See ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 80. See also Council of Advisers (2021), *The Council Of Advisers' Report On The Application Of The Rome Statute Of The International Criminal Court To Cyberwarfare*, pp. 26–36.
24 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field ('Geneva Convention I'), art. 49; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea ('Geneva Convention II'), art. 50, Geneva Convention relative to the Treatment of Prisoners of War, art. 129; Geneva Convention relative to the Protection of Civilian Persons in Time of War, art. 146; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts ('Additional Protocol I'), art. 85.

many other violations of these treaties amount to war crimes under customary international law. Article 8 of the ICC Statute sets out a long list of war crimes, and this is incorporated into the national law of many states.[25] Other states have their own shorter – or in some cases, longer – lists.[26]

The long list of war crimes set out in the Rome Statute is divided into war crimes committed in international armed conflict (between states) and those committed in non-international armed conflict (involving at least one non-state armed group). The list for international armed conflict includes 'grave breaches' of the Geneva Conventions such as wilful killing, torture or inhuman treatment, and wilfully causing great suffering. It also includes other conduct such as intentionally directing attacks against a civilian population or against individual civilians not taking direct part in hostilities, against civilian objects or, provided they are not military objectives, against religious or cultural buildings and hospitals. A war crime that should be quoted in full is 'intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated.'[27] Reference should also be made to the war crime of 'committing outrages upon personal dignity, in particular humiliating and degrading treatment'.[28]

In non-international armed conflict, serious violations such as murder, mutilation, cruel treatment, torture and committing outrages on personal dignity are war crimes. The list of other prohibited conduct is shorter than that for international armed conflict, but, as with the latter, the list includes intentionally directing attacks against a civilian population or against individual civilians not taking direct part in hostilities, and, provided they are not military objectives, against religious or cultural buildings and hospitals.

It should be stressed that the examples of war crimes given above are only a few of those listed in the Rome Statute.[29] The whole list is not set out here for reasons of space. Though the list in the statute is long, it does not include all war crimes under customary international law.[30]

It is easy to envisage a number of war crimes being committed by cyber means. Indeed, it is likely that this is now occurring.[31]

---

25 For instance, in Argentina, New Zealand and the UK.
26 See, for example, United States Code: Title 18 on Crimes and Criminal Procedure, which ties war crimes more closely to, among others, the grave breaches provisions of the 1949 Geneva Conventions. See also Ecuador's Código Orgánico Integral Penal (2014; as amended 2025), which, in article 122, provides more expansive criminal provisions on the use of weapons incompatible with IHL.
27 Rome Statute, art. 8(2)(b)(iv).
28 Rome Statute, art. 8(2)(b)(xxi) and 8(2)(c)(ii).
29 Rome Statute, art. 8 contains 59 war crimes.
30 This is particularly the case in respect of non-international armed conflict, in the view of the ICRC, on e.g. indiscriminate attacks. See ICRC (undated), 'International Humanitarian Law Databases: Rule 156', https://ihl-databases.icrc.org/en/customary-ihl/v1/rule156.
31 For example, the OTP is said to be investigating war crimes committed by cyber means in Ukraine. See Deutsch, A., van den Berg, S. and Pearson, J. (2024), 'Exclusive: ICC probes cyberattacks in Ukraine as possible war crimes, sources say', Reuters, 14 June 2024, https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14.

Terms used in certain of the definitions of war crimes need care in the cyber context. They derive from the same terms used in international humanitarian law, and therefore that body of law should be used to interpret them.[32] And, in discussing the meaning of international humanitarian law, it is relevant to look at the views taken by governments on the issue concerned. The following sections discuss those terms and the questions around them.

What constitutes an 'attack' in the cyber context?

As indicated above, some war crimes consist of unlawful 'attacks' against civilians or civilian objects. The terms 'cyber attack' and 'computer network attack' are in common use. But in international humanitarian law, 'attacks' are defined as 'acts of violence against the adversary, whether in offence or in defence.'[33] Is it possible to regard cyber operations as 'acts of violence' for the purpose of the definition of 'attack'?

Some states, and the International Committee of the Red Cross (ICRC), have made public their view that cyber operations that cause injury or death to persons, or damage or destruction of property, can be regarded as 'acts of violence' because of their *consequences* and therefore are 'attacks' for the purpose of international humanitarian law.[34] This view is now becoming well accepted.[35] It may therefore be thought likely that, if a national court were to prosecute for cyber-enabled war crimes, this would also be their approach. While this interpretation does not emerge clearly from the caselaw of the ICC, it is also the view taken in the OTP policy paper.[36]

If an 'attack' can be defined in relation to its consequences or effects, what effects are covered? The level of damage necessary to bring an operation within the definition of 'attack' is not clear. It has been described by some as needing to have similar effects to physical action constituting an attack.[37] The ICRC has stated that 'all operations expected to cause death, injury or physical damage constitute attacks, including when such harm is due to the foreseeable indirect

---

32 In seeking the meaning of terms used in IHL, the views of governments expressed in various forums may be relevant, whether found in military manuals or in statements of governments' positions on cyber operations more generally. These views may therefore also be relevant when interpreting the definitions of war crimes in the Rome Statute.
33 Additional Protocol I, art. 49(1). The ICRC adds that '[i]n other words, the term 'attack' means 'combat action'.' ICRC International Humanitarian Law Databases (undated), 'Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977: Article 49 - Definition of attacks and scope of application', para 1880, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-49/commentary/1987. See also, for example, Prosecutor v. Ongwen, Trial Judgment, 4 February 2021, ICC-02/04-01/15-1762-Red, para 2758.
34 See views given in Cyber Law Toolkit (undated), 'Attack (international humanitarian law)', https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law).
35 For some views in support, see Schmitt, M. (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, rule 92, para 3, pp. 415–16.
36 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 86.
37 See, for example, UK Government (2021), 'Application of international law to states' conduct in cyberspace: UK statement', 3 June 2021, https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/71358e6f-f834-4d09-88be-d5a13f8bf1df, para 24, arguing that '[a] cyber operation is capable of being an 'attack' under IHL where it has the same or similar effects to kinetic action that would constitute an attack.'

or reverberating effects of an attack, such as the death of patients in intensive-care units caused by a cyber attack against the electricity network that then cuts the hospital electricity supply.'[38]

Some states have pointed to the need to include 'reasonably expected' effects within the definition of 'attack'.[39] The OTP policy paper considers an attack, at the least, to cover a cyber operation 'whose (actual or potential) direct and indirect effects include death or injury to persons' or damage to civilian objects.[40]

Who is protected from 'attack'?

It is a war crime to attack civilians who are 'not taking direct part in hostilities'. A key question in the context of cyber-enabled crimes is whether the civilian cyber operators who are hired by armed forces to disable computer networks of the opposing side may be lawfully targeted. The law allows that for the duration of their direct participation in hostilities, civilians may be attacked as if they were combatants themselves.

A key question in the context of cyber-enabled crimes is whether the civilian cyber operators who are hired by armed forces to disable computer networks of the opposing side may be lawfully targeted.

While determining that a person is taking a direct part in hostilities does not require proof of the person's intent to engage in hostilities, it has been suggested that civilians 'totally unaware of the role they are playing in the conduct of hostilities' cannot be considered direct participants.[41] Depending on the facts, some employees of technology companies may have no knowledge whatsoever of the significance of their contribution to military operations.[42]

Is loss of functionality an 'attack'?

As regards attacks on civilian objects, there are a few difficult questions when the operation is in cyberspace. Is it an 'attack' – and thus a war crime – if the actual or potential effect is merely loss of functionality?

---

38 ICRC (2015), *IHL and challenges of armed conflicts*, October 2015, https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf, p. 41. See also Schmitt (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, rule 92, para 5, where the experts agreed that an attack includes not only the direct effects of a cyber operation on the targeted cyber system itself, but also *any reasonably foreseeable consequential* damage, destruction, injury or death. This was on the basis that cyber operations seldom involve the release of direct physical force against the targeted cyber system yet can result in great harm to individuals or objects.
39 Cyber Law Toolkit (undated), 'Attack (international humanitarian law)'.
40 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 86.
41 Melzer, N. (2008), *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, Geneva: International Committee of the Red Cross, p. 60.
42 van Benthem, T. J. (2023), 'Privatized Frontlines: Private-Sector Contributions in Armed Conflict', NATO CCDCOE Publications, 15th International Conference on Cyber Conflict: Meeting Reality, pp. 55–69, https://doi.org/10.23919/CyCon58705.2023.10182177, p. 63.

For at least some states and scholars, the meaning of 'attack' should be limited to acts causing physical damage.[43] But others take the view that the meaning can include disruption or loss of functionality and not just death, injury or physical damage.[44] For instance, the ICRC has argued that 'an operation designed to disable a computer or a computer network constitutes an attack under international humanitarian law, whether the object is disabled through kinetic or cyber means'.[45] On this view, examples of 'attack' would include 'disrupting or halting the functions of a state's critical infrastructure or jamming military capabilities, even if the critical infrastructure or military hardware is not physically destroyed'.[46]

The matter is still unsettled. There seems to be some agreement among experts, however, that a cyber operation may constitute an attack when the loss of functionality causes foreseeable physical damage, injury or death.[47] This is also the view taken in the OTP paper.[48] An example would be a cyber operation intended to shut down electricity in a military airfield and, as a result, cause a military aircraft to crash.[49]

Are data regarded as civilian 'objects'?

Another significant question is whether digital or electronic data can be regarded as civilian 'objects' and thus whether their destruction would amount to an 'attack' and a war crime. The OTP paper gives an example of cyber operations that delete the database of the recipients of state pensions.

Some states argue for a narrow view regarding data.[50] On this view, data are intangible and therefore cannot fall within the ordinary meaning of the term 'object'. An attack on data per se would not qualify as an attack under international humanitarian law or war crimes provisions. But a more expansive view is shared by a growing number of states.[51] And there seems to be growing agreement that

---

43 For example, Denmark, Israel and Peru. See Cyber Law Toolkit (undated), 'Attack (international humanitarian law)'.
44 See Council of Advisers (2021), *The Council Of Advisers' Report On The Application Of The Rome Statute Of The International Criminal Court To Cyberwarfare*, para 12, p. 38. See also ICRC (2019), *ICRC Position Paper on International Humanitarian Law and Cyber Operations during Armed Conflicts*, Geneva: International Committee of the Red Cross, https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf.
45 ICRC (2021), 'International humanitarian law and cyber operations during armed conflicts: ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019', *International Review of the Red Cross*, 102(913), pp. 481–92, https://doi.org/10.1017/S1816383120000478, p. 489.
46 Council of Advisers (2021), *The Council Of Advisers' Report On The Application Of The Rome Statute Of The International Criminal Court To Cyberwarfare*, para 12. The Tallinn Manual 2.0 experts were divided on the question. A majority considered that damage includes interference with functionality if restoration of functionality requires the replacement of physical components. For some experts, damage would also extend to situations where the system needs to be reinstalled to perform its original functions. See Schmitt (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, rule 92, paras 10–12.
47 Schmitt (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, rule 92, para 15.
48 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 90.
49 Schöndorf, R. (2020), 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', *International Law Studies*, 97(1), pp. 400–01, https://digital-commons.usnwc.edu/ils/vol97/iss1/21.
50 For example, Denmark, Chile and Israel. See Cyber Law Toolkit (undated), 'Military Objectives – Qualification of data as an object under IHL', https://cyberlaw.ccdcoe.org/wiki/Military_objectives#Qualification_of_data_as_an_object_under_IHL. This was also the view of the majority of Tallinn Manual 2.0 experts, who agreed that 'the law of armed conflict notion of 'object' is not to be interpreted as including data, at least in the current state of the law.' See Schmitt (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, rule 100, para 6. See also Pomson, O. (2023), "Objects'? The Legal Status of Computer Data under International Humanitarian Law', *Journal of Conflict & Security Law*, 28(2), pp. 349–87, https://doi.org/10.1093/jcsl/krad002.
51 For example, Austria, Finland, Germany, Norway and Romania. See Cyber Law Toolkit (undated), 'Military Objectives - Qualification of data as an object under IHL'; Austrian Position, p. 18.

a cyber operation directly targeting data may qualify as an attack if, at the very least, it results in physical damage, injury or death. The ICRC has noted that:

> the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them. Excluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap.[52]

The protection of civilian data is grounded in the idea that even electronic data have a physical existence – data are physically stored in a computer server located somewhere. All forms of data are recorded or contained in a physical substratum – whether in a computer chip or a piece of paper. The OTP paper does not take a view on whether data alone can qualify as an 'object', while agreeing that deletion of data that could lead to death of civilians or damage to a civilian object could constitute a war crime.[53]

Are dual-use items covered?

An issue arises when an object has a *dual* use – i.e. it can be used for both civilian and military purposes. International humanitarian law allows the targeting of military objectives.[54] It is an attack on civilian objects that constitutes a war crime. Civilian ICT networks are also used by the military, and the computer systems of civilians and the military are often interconnected. But an assessment that such dual-use items are all military objectives and may thus be lawfully targeted could render vacuous the principle of distinction between civilian and military, which is at the heart of international humanitarian law.

An assessment that dual-use items are all military objectives and may thus be lawfully targeted could render vacuous the principle of distinction between civilian and military, which is at the heart of international humanitarian law.

Assessments will have to be made on a case-by-case basis. It may be that attacks on dual-use objects that have an indiscriminate and disproportionate impact on the civilian population, undertaken with the relevant knowledge and intent, may be prosecuted as attacks on civilians. This is at least the case, according to the OTP paper, 'when it is technically possible to isolate and target only the military objective and the perpetrator intentionally declined to do so'.[55]

---

52 ICRC (2021), 'International humanitarian law and cyber operations during armed conflicts', p. 490. The ICRC analogy with paper files is perhaps simplistic. Digital data are transient and can simultaneously reside across multiple systems.
53 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 91. The OTP will bear in mind 'the evolving practice and positions of States' on the qualification of data as an object.
54 Military objective is defined in Addition Protocol 1 to the Geneva Conventions as 'those objects which by their nature, location, purpose or use make an effective contribution to military action' and whose destruction 'offers a definite military advantage.' (Art. 52(2)).
55 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 88. There is some support in ICC caselaw for the proposition that indiscriminate attacks (not as such a crime in the ICC Statute) can be prosecuted as attacks against civilians – *Prosecutor v Katanga* (Trial Chamber Judgment) ICC-01/04-01/07 (7 March 2014), para 802.

2.4 Aggression

Example

Leaders of a state with territorial ambitions over a neighbouring state order their military to launch computer network attacks against the systems used by the neighbouring state's military aircraft and warships, leading to crashes and deaths.

As defined in the Rome Statute, the crime of aggression means 'the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations.'

The statute then provides a list of 'acts of aggression'. The list includes: invasion or attack by the armed forces of a state in the territory of another state; attack on their forces; any military occupation or annexation by the use of force; blockade of ports by the armed forces of another state; allowing one's territory to be used by another state to commit an act of aggression against a third state; and the 'sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein'.[56]

While these categories were agreed without regard to the use of cyber operations, they should be interpreted as including the use of any means, including cyber ones. The example given in the box above of an attack on another state's military aircraft and ships would come within the definition of an act of aggression.

But such an act would not amount to the crime of aggression under the Rome Statute unless it met the threshold of a 'manifest violation' of the UN charter by reason of its 'character, gravity and scale'. The term 'manifest violation' is intended to exclude acts that are not clearly unlawful. The criteria of gravity and scale may be applied by reference to the campaign as a whole, and not simply to the cyber elements of it. The OTP paper says that 'as a practical matter it presently may be more likely that cyber operations will be used by the aggressor state as part of a wider course of conduct, also including acts entailing physical or kinetic force.'[57]

No prosecutions for aggression have yet been instituted by the ICC. Because of the particular characteristics of the crime – the responsibility of the state for a 'manifest violation' of the law on the use of force, committed by leaders – and stricter criteria

56 The list is taken from Article 3 of the UN General Assembly's Definition of Aggression (GA res.3314 (XXIX), 14.12.1974 with the Definition of Aggression annexed to it).
57 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 100.

for the ICC to take jurisdiction,[58] future cases in the ICC will perhaps be infrequent. But aggression is criminalized in the legislation of some individual states, and it may also be prosecuted in ad hoc tribunals.[59]

2.5 The mental element of international crimes

Most international crimes require that the relevant acts were committed *intentionally*.[60] Under the Rome Statute, the default mental element is set at 'intent and knowledge'.[61] While domestic legal systems can establish mental elements lower than intent, the gravity of the label 'international crime' militates against lowering standards to liability without fault.

The use of ICTs can both assist the proof of intent and open the possibility for unintended harms. As an example of the first, the Stuxnet malware that caused damage to Iran's nuclear programme was designed for impact on industrial control systems. It would therefore be difficult to argue that its impact was unintended. As an example of the second, it is possible for cyber operations to affect networks in ways not desired or foreseen by their deployers. For example, the NotPetya wiper cyberattack, which was seemingly meant to target Ukrainian banks, airports and energy companies, instead spread globally and affected over 2,300 organizations in over 100 countries.[62]

When ICTs are coupled with the use of AI, the risk of unintended harms becomes even greater. Whether AI is integrated into autonomous weapons systems (i.e. systems selecting and engaging targets without human intervention) or decision-support systems (i.e. those used to support human decision-making), the operation of the system may be relatively unexplainable, unpredictable and untraceable to its deployers. In practice, this means that individuals operating AI systems may not fully foresee the processes or consequences of the tools they use. For instance, an operator using an AI-powered programme for the identification of military networks may have limited time to act between receiving a list of identified networks and approval for engagement, and may be unable to verify how the AI system reached its conclusions. If the system then engages a civilian network, it is unlikely that the operator would be liable for the international crime of directing attacks against civilian objects, as they neither intended that outcome nor foresaw it.[63] Further, it is also conceivable

---

58 Rome Statute, arts 15*bis* and *ter*.
59 The crime of aggression has been introduced in the domestic law of, among others, Denmark, Guinea, Honduras, Poland, Russia, Ukraine and Vietnam. As regards ad hoc tribunals, a Special Tribunal for the Crime of Aggression against Ukraine was established in June 2025 via agreement between the Council of Europe and Ukraine. See Council of Europe (2025), 'CM(2025)104-final - [1532/2.3] Consequences of the aggression of the Russian Federation against Ukraine, Agreement between the Council of Europe and Ukraine on the Establishment of the Special Tribunal for the Crime of Aggression against Ukraine', 24 June 2025, https://search.coe.int/cm?i=0900001680b678c9.
60 However, intent is not always required. For instance, the customary war crime of directing attacks against civilians can be committed with both intent and recklessness (*Prosecutor v Galic* (ICTY Appeals Chamber Judgement) IT-98-29-A (30 November 2006), para 140). Further, the Rome Statute crime of conscription of children under the age of 15 only requires negligence in relation to age (Rome Statute, Elements of crimes, art. 8(2)(b)(xxvi)).
61 Rome Statute, art. 30.
62 Poireault, K. (2023), 'What Have We Learned from NotPetya Six Years On?', InfoSecurity Europe, 11 July 2023, https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/learnings-from-notpetya-cyberattack.html.
63 van Benthem, T. (2024), 'Symposium on Military AI and the Law of Armed Conflict: Responsible Deployments of Militarised AI – The Power of Information to Prevent Unintended Engagements', Opinio Juris, 2 April 2024, https://opiniojuris.org/2024/04/02/symposium-on-military-ai-and-the-law-of-armed-conflict-responsible-deployments-of-militarised-ai-the-power-of-information-to-prevent-unintended-engagements.

that an AI system could self-initiate and cause harm without any intent on behalf of its human operators to engage in an act of violence. This, in turn, raises the question whether such self-initiation can constitute an 'attack' under the war crimes regime, given that it was not performed deliberately.[64]

While AI systems can be used as a tool to commit international crimes in much the same way as any other, difficult questions arise when the operation of the AI system is unforeseeable or unexplainable to its human operators and supervisors. Unless those individuals are *aware* that their weapon mischaracterizes civilians and civilian objects as lawful military objectives, there may be limited scope for individual responsibility under international criminal law.

2.6 Offences against the administration of justice

Just as states include in their national law offences to preserve their justice systems from obstruction and interference,[65] so the Rome Statute includes 'offences against the administration of justice'. These offences include conduct such as giving false evidence, tampering with witnesses or evidence, and hampering the administration of justice in other ways.[66] It is easy to envisage these offences being committed by cyber means – including tampering with evidence and witness interference by the use of digital deepfakes, for example.[67]

2.7 Participation in the commission of international crimes

Under the Rome Statute, as well as in domestic legal systems, individuals can be held criminally responsible not only when they physically pull the trigger or press the computer key, but also when their conduct constitutes another form of participation in a crime. This could be ordering, inducing, attempting, facilitating or – under some circumstances – failing to prevent a crime or punish its perpetrators. How the boundaries of these forms of participation are drawn depends on the relevant legal framework.

This section provides an overview of the main forms of criminal participation in international criminal law, with specific reference to the use of ICTs. It focuses on the prosecution of cyber-enabled international crimes by the ICC, drawing

---

64 For a discussion of the concept of 'attack', see p. 14. On the concept of attack and its interaction with conduct of hostilities obligations, see van Benthem, T. (2021), 'The redirection of attacks by defending forces', *International Review of the Red Cross*, 102(914), pp. 875–92, https://doi.org/10.1017/S1816383121000679.
65 For instance, the UK Criminal Justice and Public Order Act 1994 contains offences against witnesses and jurors, including their harming and intimidation.
66 Rome Statute, art. 70(1). The Rome Statute criminalizes six different forms of conduct against the administration of justice.
67 It should be noted that the ICC has itself been the target of harmful cyber operations, in 2023 and 2025. See ICC (2023), 'Measures taken following the unprecedented cyber-attack on the ICC', press release, 20 October 2023, https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc; and ICC (2025), 'ICC detects and contains new sophisticated cyber security incident' press release, 30 June 2025, https://www.icc-cpi.int/news/icc-detects-and-contains-new-sophisticated-cyber-security-incident.

on existing caselaw from the ICC and previous international criminal tribunals, such as the ICTR and the International Criminal Tribunal for Yugoslavia (ICTY). It also addresses the ways various states incorporate and implement international criminal law through their own domestic law. Each domestic legal system contains its own regulation of forms of participation in criminal conduct, and these sometimes differ from those in international law.

The use of ICTs can, on the one hand, further obscure the link between individual contribution and harm by stretching chains of causation between individual conduct and a harmful outcome. But, on the other, it can clarify the roles that individuals play by providing a retrievable digital footprint of their conduct.

International criminal law is geared towards the regulation of collective criminality and large-scale harms, where the causal relationship between individual conduct and a particular harmful outcome is not always easy to discern.[68] The use of ICTs can, on the one hand, further obscure the link between individual contribution and harm by stretching chains of causation between individual conduct and the manifestation of a harmful outcome. But, on the other hand, ICT use can clarify the roles individuals play by providing a retrievable digital footprint of their conduct.

In practice, the relationship between cyber and physical conduct in the commission of international crimes can take various forms. There can be physical *and* cyber forms of participation in the commission of cyber-enabled crimes. Crimes which are committed by physical means can be ordered, induced or facilitated through cyber means. And conduct committed on or via ICTs could provide useful evidence to prove elements relevant for particular forms of participation, such as knowledge of circumstances or consequences.

The main forms of criminal participation are:

Perpetration

An individual can commit a crime on their own, jointly with, or through, another person.[69] For instance, an individual who, in the context of an armed conflict, intentionally deploys ransomware to lock hospital staff out of their systems and prevent the delivery of emergency care could be responsible as a direct perpetrator for the crime of intentionally directing attacks against civilians or civilian objects. Where there is more than one perpetrator, each co-perpetrator's contribution must be essential for the crime to have been committed in the way that it was. The co-perpetrators must also share a common criminal plan. Within such a framework of shared intent, in the context of ICTs, the tasks of development and deployment

68 Ambos, K. (2021), 'Individual criminal responsibility', in Ambos, K. (2021) (ed.), *Rome Statute of the International Criminal Court: Article by Article Commentary*, 4th edn, London: Beck/Hart/Nomos, p. 1197.
69 Rome Statute, art. 25(3)(a).

of malware could be spread among multiple individuals – one actor could be scanning for vulnerabilities in target systems, another coding the malware and a third deciding on the timing of its employment.

Commission 'through another person' establishes a form of responsibility in cases where an indirect perpetrator commits the crime by controlling the will and acts of another (or others), irrespective of whether that latter person (or persons) is responsible (a 'perpetrator behind the perpetrator') or not (an 'innocent agent').[70] Indirect perpetration can be of particular relevance in the context of ICTs. Criminals using ICTs often exploit unknowing persons through forms of social engineering, such that these unknowing persons themselves trigger the causal chain of harm.

The caselaw of the ICC has affirmed that indirect perpetrators can commit crimes by exercising control over an organization,[71] evidenced by the establishment of a system of automatic compliance (through strict training, payment and punishment mechanisms, among others) and relative interchangeability of the 'instruments' of the indirect perpetrator.

Although many hacker collectives are loosely organized and coordinated, certain cybercriminal groups may bear the hallmark of organizations with strict compliance systems and interchangeability of affiliates. Little is known of the precise parameters within which cybercriminal groups operate. However, for example, it has been revealed that dark0de – a black-market website for cybercrime – operated on an invite-only basis, with members being subject to rigorous vetting and a system of promotions once admitted.[72]

One challenge in applying doctrines of perpetration to the ICT context relates to the use of AI tools. Humans may have limited foresight of or control over the functioning of an AI model, or they may be part of a system of human–machine interaction in which their meaningful supervision is eroded due to time pressures or cognitive biases such as automation bias (i.e. when humans 'over-trust' the outcome of a machine process). As explained in section 2.5, if the harmful outcome of the AI application was unintended, this may mean that no international crime was committed. Of course, if humans intentionally use AI to torture, persecute, target civilians and civilian objects, criminal responsibility is clear.

Ordering

When an individual orders the commission of a crime, they are using their position of authority to convince or coerce another to commit that crime.[73] What is implied in this form of participation, therefore, is a form of superior–subordinate relationship.[74] Orders can be transmitted through both physical and digital means. Thus, an order can be made via ICTs – for example, by a text message.

---

70 Kiss, A. (2019), 'Indirect Commission', in de Hemptinne, J., Roth, R. and van Sliedregt, E. (eds) (2019), *Modes of Liability in International Criminal Law*, Cambridge: Cambridge University Press, pp. 30–57, para 59.
71 ICC, *Prosecutor v. Ongwen*, Judgment on the appeal of Mr Ongwen against the decision of Trial Chamber IX of 4 February 2021 entitled 'Trial Judgment', 15 December 2022, ICC-02/04-01/15-2022-Red A, paras 626–34.
72 Williams, D. (2024), 'How High Level Cybercrime Groups Are Formed and Organized', BLACKFOG, 24 June 2024, https://www.blackfog.com/how-high-level-cybercrime-groups-are-formed.
73 *Prosecutor v Akayesu* (ICTR Trial Judgment) ICTR-96-4-T (2 September 1998), para 483.
74 *Prosecutor v Mudacumura* (ICC Pre-Trial Chamber II Decision on the Prosecutor's Application under Article 58) ICC-01/04-01/12-1Red (13 July 2012), paras 63–65.

Soliciting and inducing

Soliciting and inducing cover similar conduct characterized by the urging or otherwise inciting of another person to commit a crime, but without a relationship of authority. According to ICC caselaw, inducement is a stronger form of instigation compared to solicitation. While solicitation is, at base, about asking or urging the physical perpetrator to commit the criminal act, inducement requires exertion of influence over the physical perpetrator, 'either by strong reasoning, persuasion or conduct implying the prompting of the commission of the offence'.[75] The acts of inducement and solicitation must have had a direct effect on the commission or attempted commission of the crime.

Inducement and solicitation can occur through psychological pressure or manipulation, among other methods, and can find wide application to the harmful information operations proliferating on social media. For example, the Independent International Fact-finding Mission on Myanmar found in 2018 that Facebook had been 'a useful instrument for those seeking to spread hate' against the Rohingya, including Myanmar's authorities.[76] While online incitement by the Myanmar authorities could also plausibly be characterized as direct and public incitement to genocide,[77] the forms of participation of inducement and solicitation are broader, as they can relate to any international crime.[78] For example, they could cover orchestrated social media campaigns that incite their audiences to commit the crimes against humanity of rape and torture, or the war crimes of destruction and appropriation of property.

Assistance

There is criminal responsibility in cases where individuals assist the commission of an international crime. This complicity rule has a wide scope, covering any act that contributes to the commission or attempted commission of a crime – be it a physical or psychological type of support, in the form of an action or omission. Moral support and encouragement – including, in certain circumstances, mere presence at the scene of the crime – can constitute acts of assistance under this mode of liability.[79] Such assistance can occur before, during or after the commission of the principal crime.[80] The assisting party need not know all

---

75 *Prosecutor v. Bemba et al* (ICC Judgment pursuant to article 74 of the Statute) ICC-01/05-01/13-1989-Red (19 October 2016), para 76.
76 UN Human Rights Council (2018), *Report of the independent international fact-finding mission on Myanmar* (A/HRC/39/64), 10–28 September 2018, https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/FFM-Myanmar/A_HRC_39_64.pdf, paras 35; 73–74. Following the UN panel's report, Facebook commissioned its own independent report on the matter that acknowledged that the company needed to do more to prevent its 'platform from being used to foment division and incite offline violence'. It pledged to reform its processes and take further actions to prevent such uses of the platform in future. See Warofka, A. (2018), 'An Independent Assessment of the Human Rights Impact of Facebook in Myanmar', article, Facebook, 5 November 2018 (updated 26 Aug. 2020), https://about.fb.com/news/2018/11/myanmar-hria.
77 See p. 10.
78 An important difference between direct and public incitement to genocide and inducement/solicitation is that while incitement to genocide is an inchoate crime, that is, no resulting genocide is required (see section 2.1, above), inducement and solicitation are modes of liability whereby the relevant crime must actually be attempted or committed. See also Ambos, K. (2021), 'Criminal responsibility, Modes of', in Peters, A. (ed.) (2021), *Max Planck Encyclopedia of Public International Law*, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1853.
79 *Prosecutor v Furundžija* (ICTY Trial Chamber Judgment) IT-95-17/1-T (10 December 1998), paras 190–249.
80 *Prosecutor v. Bemba et al* (ICC Public redacted version of Judgment pursuant to Article 74 of the Statute) ICC-01/05-01/13-1989-Red (19 October 2016), para 96.

the details of the crime in which they assist,[81] or, in certain domestic systems, even the precise crime.[82]

Given the virtually unlimited range of acts captured by 'assistance', the courts have developed limiting factors. First, the act of assistance must have an *effect* on the commission of the offence – whether that effect has to represent a 'substantial' contribution to the crime,[83] or create or increase the risk that the crime will be committed,[84] or otherwise facilitate or further the commission of the crime.[85] Another limiting factor is that the contribution of the accomplice must be made 'for the purpose of facilitating' the commission of a crime. This rather high requirement is not always to be found in domestic systems. In the UK, for example, it is sufficient for the assisting party to intend to assist the commission of the crime. It is not necessary to prove that the accomplice *wanted* the crime to be committed – indeed, they can be indifferent to its commission.

The complicity rule has a wide scope, covering any act that contributes to the commission or attempted commission of a crime – be it a physical or psychological type of support, in the form of an action or omission.

In the context of ICTs, it has been argued that information operations disseminated online and aimed at the concealment of the truth about international crimes and/or obstruction of accountability can, subject to satisfying the relevant subjective and objective elements, qualify as criminal acts of assistance under the Rome Statute.[86] The ICC has accepted that *ex post facto* assistance can trigger assistance liability in circumstances where, following an offer of assistance or agreement with the accomplice, the principal perpetrator committed the crime knowing they would receive assistance in the aftermath.[87]

---

81 *Prosecutor v. Bemba et al* (ICC Judgment on the appeals of Mr Jean-Pierre Bemba Gombo, Mr Aimé Kilolo Musamba, Mr Jean-Jacques Mangenda Kabongo, Mr Fidèle Babala Wandu and Mr Narcisse Arido against the decision of Trial Chamber VII entitled 'Judgment pursuant to Article 74 of the Statute') ICC-01/05-01/13-2275-Red A A2 A3 A4 A5 (8 March 2018), para 1400.
82 UK, *DPP for Northern Ireland v. Maxwell* [1978] 1 W.L.R. 1350 HL, paras 10, 14–15, 90. Similarly, in France, the doctrine of assistance falls within the broader umbrella of 'complicity', which captures 'a person who knowingly, through aiding or abetting, has facilitated the preparation or commission of a crime'. See Code Pénal, art. 121–27.
83 *Prosecutor v Rutaganda* (ICTR Trial Chamber I Judgment) ICTR-96-3-T (6 December 1999), para 43.
84 Ambos, 'Individual criminal responsibility' in Ambos (2021) (ed.), *Rome Statute of the International Criminal Court: Article by Article Commentary*, p. 1224.
85 *Prosecutor v. Bemba et al* (ICC Judgment on the appeals of Mr Jean-Pierre Bemba Gombo, Mr Aimé Kilolo Musamba, Mr Jean-Jacques Mangenda Kabongo, Mr Fidèle Babala Wandu and Mr Narcisse Arido against the decision of Trial Chamber VII entitled 'Judgment pursuant to Article 74 of the Statute') ICC-01/05-01/13-2275-Red A A2 A3 A4 A5 (8 March 2018), para 1327.
86 Jordash, W. et al. (2025), *Manufacturing Impunity: Russian Information Operations In Ukraine, Russia's Use of Information Alibis and How They Materially Contribute to the Planning, Execution and Cover-up of International Crimes*, report, Global Rights Compliance and The Reckoning Project, https://globalrightscompliance.org/wp-content/uploads/2025/05/Manufacturing-Impunity.pdf, p. 108.
87 *Prosecutor v. Bemba et al* (ICC Appeals Judgment), para 1399. On ex post facto assistance in international criminal law, see further Jackson, M. (2015), *Complicity in International Law*, Oxford: Oxford University Press, pp. 73–75.

Another question of great practical significance is whether the CEOs of digital service providers – and, in particular, social media platforms – can be criminally responsible for assisting the commission of international cyber-enabled crimes. The provision of a 'space' in which hateful rhetoric can spread and subsequently manifest in the physical world through violent action, together with the use of algorithms that prioritize and amplify such speech, could potentially be regarded as an act of assistance. Depending on the circumstances, it may produce the relevant effect on the commission of crimes. In many cases, however, this assistance will not be provided with the necessary intent, especially for the 'purpose of facilitating' test under the Rome Statute. There will therefore be no criminal responsibility.

It is not difficult nevertheless to imagine circumstances in which digital service providers may be deemed as acting with the necessary intent. For example, if an authoritarian leader pursues the development of 'home-grown' providers to facilitate the criminal policies of their regime, the CEOs of such providers may indeed be responsible for criminal assistance.

Contribution to criminality of a group of persons acting with a common purpose

This form of participation in criminal conduct targets contributions to collective attempts at criminality, where the collective – the group – acts with a common purpose. According to ICC caselaw, the contribution must meet a test of significance – 'it cannot be just any contribution'. But, at the same time, there is 'no additional requirement for a certain level of contribution or threshold to be attained'.[88] The individual making the contribution need not be part of the group: they can be external to its organization.[89] In terms of subjective elements, on one level, the participant must make an intentional contribution, and, on another, they must either contribute 'with the aim of furthering the criminal activity or criminal purpose of the group', or do so 'in the knowledge of the intention of the group'.[90]

This form of accessorial liability can be of particular relevance to cyber contributions – including geographically and causally distant ones – that are meant to or known to advance the group's criminal activity. For instance, imagine an individual who is aware of a group's intent to target the water filtration facilities of a state with malware, gain access to their networks and increase the levels of dangerous chemicals in drinking water. That individual aims to further the criminal activity of the group, and, in the days prior to the targeting of the water filtration facilities, overwhelms their networks with a distributed denial of service (DDoS) attack, making them unavailable to the facilities' employees.

This kind of 'common purpose' participation in a crime is dealt with in various ways in national systems. In South Africa, common purpose liability exists in the form of both prior express or implied agreement between parties to commit an offence or of active association with the commission of an offence. Under active association, it is sufficient to prove that the individual foresaw the possibility that others may commit a crime to further the group's purpose, and reconciled themselves with

88 *Prosecutor v. Al Hassan* (ICC Trial Judgment) ICC-01/12-01/18-2594-Red (26 June 2024), paras 1240–244.
89 *Prosecutor v. Mbarushimana* (PTC I Decision on the confirmation of charges) ICC-01/04-01/10-465-Red (16 December 2011), paras 274–75.
90 Rome Statute, art. 25(3)(d).

that eventuality.[91] In the UK, individuals can be held liable for conspiracy when two or more persons agree to commit a crime, regardless of whether the crime is actually committed.[92]

Common purpose liability, though apt to cover conduct assisting ICT-enabled crimes, can also become unbounded, if not constrained with appropriate standards for a guilty mind. In the UK, for example, after some caselaw suggesting that criminal responsibility for joint criminal enterprise can be established on the basis of foresight of the possible commission of an offence,[93] the law was changed to cover only intentional support by words and deeds to the commission of the crime.[94] Both the ICC and national courts should be wary of expansive common purpose liability doctrines that come in tension with individual culpability.

Superior responsibility

The Rome Statute incorporates the doctrine of superior responsibility,[95] which criminalizes certain omissions of 'superiors' with respect to criminal acts or omissions of their subordinates. Superiors are not only individuals in the military chain of command, but also civilian superiors exercising effective control. For example, in the ICTR case regarding RTLM, Nahimana was found guilty of direct and public incitement to commit genocide by virtue of his position as a 'superior' at the radio station. He was actively engaged in the management of the organization and failed to take necessary and reasonable measures to prevent the killing of Tutsi civilians instigated by the radio station's personnel.[96]

Heads of social media companies and other digital service providers could similarly be held responsible as civilian superiors for wrongful omissions in relation to the criminal conduct of their subordinates.

Superior responsibility is contingent on the presence of four elements:

1. **Existence of a subordinate crime.** If there is no crime by a subordinate, there is no superior responsibility. So, for example, if subordinates are unable to anticipate the effects of the ICT tools they deploy, they will not have the necessary *intent* to commit a crime: the subordinates will not have committed a crime, and neither will their superiors have criminal responsibility.
2. **Superior–subordinate relationship.** A superior–subordinate relationship exists when a superior exercises effective control over their subordinates, with the ability to prevent and punish subordinate acts.[97] Establishing such control may be more difficult with respect to individuals without formal ties to the commander or superior, such as members of loosely organized hacker collectives or cyber volunteers. Furthermore, under the Rome Statute, where the superior–subordinate relationship is not of a military or paramilitary

91 Constitutional Court of South Africa, *Thebus and another v the State*, CCT 36/02, 20 February 2003; Supreme Court of Appeal of South Africa, Govender v The State, ZASCA 60, 3 May 2023.
92 Criminal Law Act 1977, Part I – Conspiracy.
93 *R v Powell and R v English* [1999] 1 AC 1. See also, at the Privy Council, *Chan Wing-Siu v The Queen* [1985] AC 168.
94 *R v Jogee* (Appellant) [2016] UKSC 8.
95 Rome Statute, art. 28.
96 *Prosecutor v Nahimana et al* (ICTR Appeals Chamber Judgment) ICTR-99-52-A (28 November 2007), paras 785–857.
97 *Čelebići* (ICTY Trial Chamber Judgement) IT-96-21-T (16 November 1998), paras 377–78; *Čelebići* (ICTY Appeals Chamber Judgement) IT-96-21-A (20 February 2001), paras 197, 256.

nature, the subordinate's crimes must have 'concerned activities that were within the effective responsibility and control of the superior'.[98] In other words, the subordinate's crimes must have occurred in the context of their relationship with the superior, rather than being a private matter of their own.

3. **Fault.** For military commanders, the crime is committed if the superior 'knew or, owing to the circumstances at the time, should have known',[99] and for civilian superiors, if they 'knew, or consciously disregarded information'.[100] In complex organizational systems, such as the malware-as-a-service criminal ecosystem, persons formally or factually controlling and overseeing the process might have a fragmented understanding and knowledge of the conduct of all relevant actors, which could include 'malware developers and operators, affiliates, analysts, botmasters, initial access merchants, money processing and laundering specialists, escrow services, forum and illicit marketplace administrators, infrastructure administrators, [and] even negotiation and customer support personnel'.[101] In such structures, even the constructive knowledge standard of 'should have known' could be difficult to meet.
4. **Failure to take measures to prevent or punish the perpetrators of the principal crime.** This requires the adoption of necessary and reasonable measures: the superior is not asked to perform the impossible. What is 'necessary' and 'reasonable' is fact dependent. It depends, among others, on the extent of the superior's actual and proven material ability to act to prevent or punish those crimes.[102]

Many domestic systems – including those of Bosnia and Herzegovina,[103] Chile,[104] the Democratic Republic of the Congo[105] and France[106] – incorporate variants of superior responsibility. However, not all states (fully) incorporate superior responsibility for international crimes in their national law.

Attempt

Attempt is the taking of action that 'commences [a crime's] execution by means of a substantial step', to use the wording of the Rome Statute. For attempted crimes in, or otherwise involving, cyberspace, it may be unclear when execution commences and what constitutes 'a substantial step'. For example, would the writing of a certain piece of code be sufficient, or would the code need to be tested or verified, triggered

---

98 Rome Statute, art. 28(2)(b).
99 Rome Statute, art. 28(1)(a).
100 Rome Statute, art. 28(2)(a).
101 Bátrla, M. and Harašta, J. (2022), '"Releasing the Hounds?" Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations', NATO CCDCOE Publications, Proceedings of the 14th International Conference on Cyber Conflict, p. 96.
102 *Prosecutor v. Bemba* (ICC Judgment on the appeal of Mr Jean-Pierre Bemba Gombo against Trial Chamber III's 'Judgment pursuant to article 74 of the Statute') ICC-01/05-01/08-3636-Red (8 June 2018), paras 167–70; *Aleksovksi* (ICTY Trial Chamber Judgment) IT-95-14/1-T (25 June 1999), para 78; Strugar (ICTY Trial Chamber Judgment) IT-01-42-T (31 January 2005), para 378.
103 Krivični Zakon Bosne i Hercegovine [Criminal Code of Bosnia and Herzegovina] (2003, as amended through 2023), art. 180, Individual and Command Responsibility.
104 Ley núm. 20.357, por la que se tipifican los crímenes de lesa humanidad, el genocidio y los crímenes de guerra [Law 20.357 defining crimes against humanity, genocide and war crimes] (2009), art. 35.
105 Code Pénal (Loi n.15/022 du 31 décembre 2015, modifiant le Code Pénal) [Criminal Code, and Law of 2015 amending the Criminal Code], art. 22 bis.
106 Code Pénal [Criminal Code], Chapitre III: Dispositions communes, art. 213-4-1.

or even directed at a target? Given advances in cybersecurity and cyber defence, many potentially harmful cyber operations will be averted. The offence of attempt can therefore gain a particular significance. This, in turn, highlights the need for its further clarification.

States play a crucial role in the implementation of international criminal law and sometimes regulate forms of criminal participation in ways that differ from the Rome Statute.

The typical suspect before the ICC is likely to be the person who orders, plans or otherwise takes part in criminality at a mid- or high level – not the low-level hacker physically pressing a key. Domestic systems do not face such constraints. States play a crucial role in the implementation of international criminal law and sometimes regulate forms of criminal participation in ways that differ from the Rome Statute. As explained above, the forms of criminality established at the domestic level can track the Rome Statute formulations or be broader or narrower. An example of a mode of participation that goes beyond what is established in the Rome Statute is the Bulgarian Criminal Code's crime of justification, denial or underestimation of an international crime: 'whoever, in whatever manner, justifies, denies or seriously underestimates a crime against peace and humanity and by doing so creates a risk of expression of violence or hatred […] shall be punishable by imprisonment from one to five years.'[107] While this provision can be interpreted as a self-standing offence, it can also be conceptualized as a form of assistance in international criminality.

As discussed in Chapter 3, how states incorporate international law domestically, and the standards for substantive crimes and forms of participation they establish in their domestic law, are critical to the way in which accountability for international crimes can be implemented.

2.8 Avoidance of criminality

One does not simply stumble into international criminality. At the same time, the variety of modes of participation in international crimes under both the Rome Statute and domestic law places certain individuals within organizational structures at particular risk of criminal involvement. This is particularly true for military superiors and the leadership of large corporations, including ICT companies.

To avoid criminal complicity in the wrongs of others, and to prevent wrongs whose commission could have been avoided, specific measures need to be taken and protocols put in place. Irrespective of whether crimes are committed by cyber or other means, well-regulated militaries will already have in place measures both to avoid the commission of war crimes by their personnel and to ensure that those

107 Наказателен кодекс на Република България [Criminal Code of the Republic of Bulgaria], art. 419a(1).

in charge do not facilitate criminality, or fail to prevent or repress it. The legal training of forces and establishment of a robust reporting and oversight system are of utmost importance.

In relation to ICT companies and other corporations, equally robust measures of governance and due diligence will need to be put in place. When the customer is in a conflict-affected area, the matter is of obvious importance. The choice of customers is hugely relevant. Measures such as escalation triggers and mechanisms for review and internal inquiry may need to be adopted. The OTP paper confirms that the office 'will investigate alleged crimes within the jurisdiction of the Court equally, irrespective whether they are committed within the context of commercial activity.'[108]

108 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 170.

03 Cyber-enabled crimes and the ecosystem of international criminal justice

Domestic and international accountability bodies form part of an ecosystem aimed at fighting impunity for international crimes.

Imagine that a military commander in state A uses a computer network in state B to launch ransomware against the healthcare system of state C, leading to a stalling in the provision of health services and the death of hundreds of civilians in need of emergency care. In which state may the commander be prosecuted for war crimes or crimes against humanity? Which states would have to be parties to the Rome Statute before the ICC could prosecute? This chapter discusses the aspects of jurisdiction that answer those questions.

It is worth emphasizing that little here is particular to cyber-enabled international crimes. States are apparently not adopting or developing cyber-specific rules and standards in the area of international criminal law, rather applying existing ones to the use of ICTs. This general discussion is nevertheless necessary before considering the practical aspects of investigation and prosecution in Chapter 4.

3.1 Investigation and prosecution by states

In the first instance, it is for states to investigate and prosecute international crimes. To be able to do so, states need to have their own domestic law in place that criminalizes the conduct concerned and gives them jurisdiction over the crimes.

National legislation

Some international treaties require states to incorporate relevant international crimes into their domestic law. This is the case for the crime of genocide and certain war crimes.[109] Most recently, the Ljubljana–The Hague Convention (adopted in 2023, but not yet in force) places an obligation on states parties to incorporate genocide, crimes against humanity, war crimes and, if notified, the crime of aggression, into their national legal systems.[110] Further, if states parties to the Rome Statute wish to retain the ability to prosecute their own nationals, rather than leaving prosecution to the ICC, they must ensure that their own law includes all Rome Statute crimes in some form or another.

Jurisdiction

First and foremost, states can legislate for conduct committed in their territory and prosecute crimes committed within their borders, regardless of the nationality of the perpetrator or victim. This 'territorial' jurisdiction may extend to crimes that are initiated abroad but are completed in that state's territory.[111]

But in the case of cyber-enabled international crimes, there may often be a question of *where* the unlawful conduct has been carried out. The concept of territory finds itself increasingly challenged by ICTs. There are technical difficulties associated with tracing where the conduct took place: hackers use a variety of tools to conceal their IP addresses, and thereby obscure the footprint of their actual location.[112] And if jurisdiction is taken on the basis of *completion* of the crime in a state's territory, cyber operations are likely to result in a wide range of cyber – and physical – effects, creating a multiplicity of states with territorial jurisdiction.[113]

As is well established in law, in some instances and for some crimes, states also assert 'nationality' jurisdiction, allowing their authorities to prosecute the state's citizens for crimes committed abroad. Beyond the nationality of the perpetrator, the nationality of the victim can also be a ground for the exercise of jurisdiction –

---

109 Genocide Convention, art. V; Geneva Convention I, art. 49; Geneva Convention II, art. 50; Geneva Convention IV, art. 146.
110 Government of Slovenia (2023), *The Ljubljana–The Hague Convention on International Cooperation in the Investigation and Prosecution of the Crime of Genocide, Crimes against Humanity, War Crimes and other International Crimes*, https://www.gov.si/assets/ministrstva/MZEZ/projekti/MLA-pobuda/konvencija-dokoncna/The-Ljubljana-The-Hague-Convention-Final-English.pdf, art. 7. Article 14 of the convention further provides an 'extradite or prosecute' obligation on states in certain circumstances. There is likely to be a new convention on crimes against humanity which would similarly include a jurisdictional provision with extraterritorial reach and an obligation to extradite or prosecute.
111 On the principle of territorial jurisdiction in cyberspace, see van Benthem, T., Kulesza, J., Sun, N. and Liu, Y. (2024), *Jurisdiction in Cyberspace*, report, Geneva: Geneva Centre for Security Policy, https://www.gcsp.ch/sites/default/files/2024-12/EWG-IL_Partnered_Jurisdiction_2024-11%3Bdigital.pdf.
112 Maillart, J. (2019), 'The limits of subjective territorial jurisdiction in the context of cybercrime', *ERA Forum*, 19, p. 375, https://doi.org/10.1007/s12027-018-0527-2.
113 Such concerns have been highlighted in the literature on this principle even without the addition of the cyber dimension. See Vagias, M. (2014), *The Territorial Jurisdiction of the International Criminal Court*, Cambridge: Cambridge University Press, ch. 6.

thus, under the 'passive personality' principle, the state of a victim's nationality can exercise jurisdiction. And, under the 'protective principle', some states exercise jurisdiction over the conduct of persons abroad which constitutes a threat to their vital interests, such as in cases of foreign threats to their national security. Because of the inter-connected nature of ICT infrastructure and the impact of vulnerabilities in digital systems of one state for the security of others, the category of 'vital interest' of the state could potentially be extended to cover certain forms of interference or threats of harm caused by cyber-enabled international crimes.

'Universal' jurisdiction allows the prosecution of crimes regardless of where they were committed and regardless of the nationality of the perpetrator or the victim. It is generally regarded as compatible with international law for states to assert universal jurisdiction over international crimes. While some states allow for universal jurisdiction even where the criminal conduct, its perpetrators and victims have no connection to that state whatsoever, others take a narrower approach, allowing prosecution only where there is some connection – for example, when the perpetrator is found in their territory.[114] At the time of writing, some 106 states worldwide provided for a form of universal jurisdiction over at least one international crime.[115]

It is generally regarded as compatible with international law for states to assert universal jurisdiction over international crimes.

There are many practical challenges associated with the exercise of universal jurisdiction. It requires the allocation of resources for crimes with little or no connection to the investigating or prosecuting state, it can be far removed from the witnesses and evidence, and it is prone to political backlash. Given these challenges, some states are seeking to establish meaningful parameters to their national regulation of the principle. For instance, Argentina, whose constitution and jurisprudence allow for 'pure' universal jurisdiction without any connection to the state, has recently issued guidelines to prosecutors for universal jurisdiction investigations that do require a link to the state, such as residency of the victim or perpetrator.[116] In Sweden, meanwhile, prosecutors need governmental approval before filing an indictment concerning international crimes committed in another state.[117]

---

114 For instance, the United Kingdom International Criminal Court Act 2001, in s. 51, limits universal jurisdiction under the act to UK residents and service personnel. However, no such limitation is required in respect of 'grave breaches'.
115 Clooney Foundation (undated), 'Justice Beyond Borders', database, https://justicebeyondborders.com/world.
116 Secretaría de Coordinación Institucional Fiscalía General de Política Criminal, Derechos Humanos y Servicios Comunitarios and Dirección General de Cooperación Regional e Internacional (2024), *Pautas Generales de Actuación del Ministerio Público Fiscal de la Nación sobre Jurisdicción Universal*, https://www.fiscales.gob.ar/wp-content/uploads/2024/12/Jurisdiccion-Universal-pautas-generales-.pdf.
117 Trial International (2020), *Universal Jurisdiction Law and Practice in Sweden*, https://www.justiceinitiative.org/uploads/550b6548-a951-425f-84b3-d75e5d78688c/universal-jurisdiction-law-and-practice-sweden.pdf.

As regards the most serious violations ('grave breaches'), the four Geneva Conventions of 1949 require states to prosecute perpetrators, wherever they are to be found and wherever the crime was committed, with extradition being an available option.[118] This requires all states to take universal jurisdiction over those crimes.

Relying on universal jurisdiction, victim groups and the organizations representing them have lodged criminal complaints in various European states – predominantly Belgium, France, Germany, the Netherlands and Sweden – for allegations of international criminality in the contexts of Gaza, Rwanda and Syria, among others.[119] Argentina has become a particularly sought-after forum for universal jurisdiction complaints, ranging from allegations of crimes against humanity committed during Gen. Francisco Franco's regime in Spain (1939–75),[120] genocide by the Myanmar leadership in relation to the Rohingya,[121] and torture through electrocution by Russian-affiliated individuals in Ukrainian territories occupied by Russia.[122]

Finally, some states have sought to assert wider – and more controversial – grounds for jurisdiction, going beyond the universally accepted grounds described above. For instance, states have sought to assert jurisdiction over certain crimes relying on the 'effects' doctrine, on the basis that conduct outside a state's territory has a substantial effect within that state's borders. For example, without clearly specifying the jurisdictional ground for doing so, the US has brought prosecutions against certain individuals suspected of committing malicious cyber operations, even in situations where the operations concerned did not take place in the US or involve a US citizen as either perpetrator or victim. In the case of *US v Stigal and Others*, the defendants were accused of hacking into 'computers associated with the Ukrainian government and entities associated with the governments of countries that provided support to the Ukrainian government in resisting Russia's invasion of Ukraine'.[123] The indictment also notes that the conspiracy included the probing of websites hosted by computers and servers that were maintained by a US government agency in Maryland, so there is some connection to the US in this case. However, the jurisdictional basis is not explicitly stated or justified.

Even if a court has jurisdiction over a particular case, there may be procedural bars to the exercise of jurisdiction. For example, immunities can be a bar to the exercise of jurisdiction by national courts. Under international law, state officials are entitled to immunity from the jurisdiction of foreign states, including foreign courts, although the extent to which this is applicable in the prosecution of international crimes is not universally agreed.[124] What this means is that persons launching operations using

---

118 Geneva Convention I, art 49; Geneva Convention II, art. 50; Geneva Convention IV, art. 146; Additional Protocol I, arts 85 and 88.
119 TRIAL International (2025), *Universal Jurisdiction Annual Review 2025*, report, https://trialinternational.org/wp-content/uploads/2025/04/03_TRIAL_UJAR_2025_FINAL_DIGITAL.pdf.
120 Márquez Velásquez, M. (2022), 'The Argentinian Exercise of Universal Jurisdiction 12 Years After its Opening', Opinio Juris, 4 February 2022, https://opiniojuris.org/2022/02/04/the-argentinian-exercise-of-universal-jurisdiction-12-years-after-its-opening.
121 Ibid.
122 Jourdan, A. and van den Berg, S. (2024), 'Exclusive: Ukraine man's torture case against Russians seeks justice in Argentina', Reuters, 16 April 2024, https://www.reuters.com/world/ukraine-mans-torture-case-against-russians-seeks-justice-argentina-2024-04-16.
123 *US v Stigal, Borovkov, Denisenko, Denisov, Goloshubov and Korchagin*, District Court of Maryland, Criminal No. LKG-24-06, 7 August 2024, https://www.justice.gov/archives/opa/media/1366441/dl.
124 States have an obligation to refrain from the exercise of jurisdiction against persons with personal immunity (reserved for the head of state, head of government and minister of foreign affairs) or functional immunity. The law is unsettled as to whether there is an exception to functional immunity for the prosecution of international crimes, but personal immunity has no such exception.

ICTs who are part of the formal apparatus of a state – such as personnel of Russia's Main Intelligence Directorate (GRU) – may seek to claim immunity because of their official functions.[125] However, members of hacker groups and isolated individuals who are not formally organs of a state (even if acting in line with that state's interests) will not have a claim to immunity from the jurisdiction of other states.

3.2 Investigation and prosecution by the ICC

Beyond the domestic courts of states lies the possibility of prosecution by the ICC. Under the Rome Statute, the ICC's jurisdiction is 'complementary' to national criminal jurisdictions.[126] States exercising jurisdiction have primacy over any corresponding ICC proceedings, provided they are genuinely able and willing to investigate and prosecute.[127]

The ICC has jurisdiction over the crimes in the Rome Statute when the relevant conduct takes place on the territory (or ships or aircraft) of a state which is a party to the Rome Statute or which has otherwise accepted the ICC's jurisdiction (an accepting state), *or* when the crime is committed by a national of a state party or accepting state.[128] The ICC does not have universal jurisdiction. Its bases of jurisdiction – territoriality and nationality – mirror those commonly taken by states for ordinary crimes. In addition, the ICC may also exercise jurisdiction if the UN Security Council refers a situation to the court by means of a resolution under Chapter VII of the UN Charter – regardless of whether any relevant state has accepted the court's jurisdiction or not.[129]

In assessing whether the relevant conduct takes place on the territory of a state party for the purpose of invoking article 12(2)(a) of the Rome Statute, the ICC has accepted that the *consequences* of conduct can also bring a case under its jurisdiction, if those consequences form part of the crime itself. In its decision authorizing an investigation into potential crimes committed against Rohingya Muslims in Bangladesh and Myanmar, the ICC explained, 'the consequence of an act of killing is that the victim dies. Both facts concerning the act and the consequence

---

125 Whether functional immunity continues to apply even where prosecution is sought for international crimes is subject to ongoing debate. See International Law Commission (2025), 'Second report on immunity of State officials from foreign criminal jurisdiction by Claudio Grossman Guiloff, Special Rapporteur', A/CN.4/780, 29 January 2025, pp. 6–18; Akande, D. and Shah, S. (2011), 'Immunities of State Officials, International Crimes, and Foreign Domestic Courts', *European Journal of International Law*, 21(4), pp. 815–52, https://doi.org/10.1093/ejil/chq080. There is no cyber-specific exception to the international law rule of functional immunity, despite isolated practice of charging foreign state agents for cyber operations under domestic law. See, for instance, US Department of Justice (2014), 'U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage', press release, 19 May 2014, https://www.justice.gov/archives/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
126 Rome Statute, preamble and art. 17.
127 An example of this provision becoming relevant arose in 2020. A preliminary investigation of the ICC prosecutor into allegations of various forms of abuse by members of UK armed forces against Iraqi civilians in detention was closed after the OTP could not conclude that the UK authorities were unwilling genuinely to carry out relevant investigative inquiries and/or prosecutions or that decisions not to prosecute in specific cases resulted from unwillingness to prosecute. See ICC Office of the Prosecutor (2020), *Final Report Iraq/UK*, 9 December 2020, https://www.icc-cpi.int/sites/default/files/itemsDocuments/201209-otp-final-report-iraq-uk-eng.pdf, para 12.
128 Rome Statute, art. 12(2)(a) and (b). The crime of aggression is subject to different jurisdictional conditions. See arts 15*bis* and 15*ter* of the Rome Statute.
129 Rome Statute, art. 13(b).

(i.e. the killing and the death)' are part of the crime. In other words, in a case where the death occurred in a state party but the act of killing did not, the ICC would have jurisdiction.[130]

Applied to the context of cyber-enabled crimes, this approach could easily become expansive. Technology knows few borders: it is spread around the world through computers, cables, satellites and other devices. Are all of the states through which a cyber operation is routed to be considered 'territorial states' for the purpose of ICC jurisdiction?

Given this 'many jurisdictions' problem in the use of ICTs, multiple states could potentially be considered as territories 'on' which an element of conduct, or the consequences of the conduct where that is a necessary part of the crime, can be said to take place – even for one, isolated cyber operation. An indication of how the ICC might approach such issues can be found in prior caselaw. In one case not directly concerning cyber-enabled crimes, the court held that 'if at least one element of a crime … or part of such a crime' is committed on the territory of a state party, that is enough.[131]

While this approach would clearly cover instances where a cyber operation is launched from the territory of state A and causes death or destruction on the territory of state B, making both A and B states on whose territory the crime took place, it would not necessarily cover states hosting cables or servers through which data transits. This view is confirmed by the OTP policy paper: the office 'would not regard the mere transit of data through a State Party's territory as a sufficient basis to assert the Court's territorial jurisdiction'.[132]

In the medium term at least, the OTP is most likely to investigate conduct in cyberspace only to the extent that it accompanies or facilitates crimes committed by physical means.

The Rome Statute was a carefully negotiated compromise, and states parties are likely to be sensitive to what could be perceived as an overexpansive approach to jurisdiction on the part of the ICC. For this reason, the ICC would be prudent to take a conservative approach to jurisdiction in cases involving cyber operations.

In addition to questions of jurisdiction, issues of immunity also arise in the operation of the ICC. While immunities are not a bar to the ICC's jurisdiction,[133] states parties to the Rome Statute may still be bound to observe the immunities of wanted individuals. The Rome Statute contains a clause protecting states parties from court

---

130 Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the People's Republic of Bangladesh/Republic of the Union of Myanmar (Pre-Trial Chamber III) ICC-01/19-27 14-11-2019 (14 November 2019), para 50.
131 *Situation in the People's Republic of Bangladesh/Republic of the Union of Myanmar*, Decision on the 'Prosecution's Request for a Ruling on Jurisdiction under Article 19(3) of the Statute' (Pre-Trial Chamber I) ICC-RoC46(3)-01/18-37 (6 September 2018), para 72.
132 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 45.
133 Rome Statute, art. 27(2).

requests that would require them to act inconsistently with their international obligations.[134] That said, ICC caselaw suggests that since immunities do not apply before the ICC itself, states parties can and must bring perpetrators to the ICC – even if the perpetrator is a sitting head of state.[135] But this approach is not without controversy.[136]

Finally, gravity is an issue not only for admissibility but also for case selection and prioritization. A case will only be heard by the ICC if it is admissible as being 'of sufficient gravity to justify further action by the Court.'[137] The OTP may apply a stricter test for assessing gravity when it chooses or prioritizes cases than is legally required for the admissibility test. In this context, its 'assessment of gravity includes both quantitative and qualitative considerations'.[138] The factors that guide the OTP's assessment include the scale, nature, manner of commission and impact of the crimes.[139] A further factor in the current policy for selection of cases is that only 'those most responsible' for the crime will be prosecuted, although this 'does not necessarily equate with *de jure* hierarchical status within a structure'.[140]

Applying the gravity criterion outlined above to cyber-enabled international crimes, it is likely that cases selected by the OTP will be those involving significant harm – such as death, injury, destruction or disruption. At the same time, even cyber-enabled crimes with few direct victims may have a significant impact through increasing the vulnerabilities of other individuals and communities. Cyber operations against critical infrastructure are one such example, as they could affect the delivery of essential services.[141] In the medium term at least, the OTP is most likely to investigate conduct in cyberspace only to the extent that it accompanies or facilitates crimes committed by physical means.[142]

---

134 Ibid., art. 98(1).
135 ICC, Situation in Ukraine, Finding under article 87(7) of the Rome Statute on the non-compliance by Mongolia with the request by the Court to cooperate in the arrest and surrender of Vladimir Vladimirovich Putin and referral to the Assembly of States Parties, ICC-01/22, 24 October 2024.
136 Akande, D. (2019), 'ICC Appeals Chamber Holds that Heads of State Have No Immunity Under Customary International Law Before International Tribunals', EJIL:Talk!, 6 May 2019, https://www.ejiltalk.org/icc-appeals-chamber-holds-that-heads-of-state-have-no-immunity-under-customary-international-law-before-international-tribunals.
137 Rome Statute, art. 17(1)(d).
138 ICC Office of the Prosecutor (2016), *Policy paper on case selection and prioritisation*, https://www.icc-cpi.int/sites/default/files/itemsDocuments/20160915_OTP-Policy_Case-Selection_Eng.pdf, paras 36–37 and 47.
139 Reg. 29(2) of the Regulations of the Office of the Prosecutor.
140 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 129.
141 Roscini, M. (2019), 'Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes', Criminal Law Forum, 30, pp. 247–72, https://doi.org/10.1007/s10609-019-09370-0, p. 268.
142 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 130.

04
Practical issues in investigation and prosecution

Cooperation between different entities (states, international organizations, private companies and civil society) will be crucial to the effective investigation and prosecution of cyber-enabled international crimes.

How prepared are states and the ICC to bring prosecutions for cyber-enabled international crimes in practice? What are the best strategies for identifying the perpetrator and gathering evidence? And what more is needed to strengthen the prospects of a successful prosecution?

This chapter looks at these issues with reference to three hypothetical scenarios, which highlight the main practical challenges and opportunities involved in the investigation and prosecution of cyber-enabled crimes. The first scenario centres on prosecution by a state, the second on prosecution by the ICC and the third on joint investigation by several states, with ICC participation. While each scenario highlights challenges specific to itself, many of the issues addressed will be relevant in all three scenarios.

4.1 Investigation and prosecution by a state

Scenario 1

A fighter in state A uses his smartphone to take graphic images and video footage of a fellow fighter beheading a journalist. He sends the video to the fellow fighter, who posts it online where it is seen by millions of people worldwide. Both fighters are captured and the smartphone seized by the authorities of state A.

This section analyses the pathways available to states to investigate and prosecute cyber-enabled international crimes, drawing on a scenario to illustrate how these pathways might apply in practice.

As noted in the previous chapter, in practice there are several barriers to states conducting such prosecutions, including lack of jurisdiction, immunities, political will and resources. However, some states have already prosecuted cyber-enabled international crimes.

Over the last decade, there have been many incidents in which fighters in war zones have filmed graphic images – for example, featuring the torture, mutilation or beheading of civilians or combatants they have captured, or the degrading treatment of dead bodies – and posted them online. As noted in Chapter 2, it is a war crime to impose inhuman treatment or to commit outrages on personal dignity, in particular humiliating and degrading treatment.[143] Some European states, whose domestic laws criminalize international crimes and provide universal jurisdiction over them, have prosecuted fighters operating in Iraq and Syria for posing in photos or videos with mutilated bodies. For example, in 2019, Oussama Akhlafa was convicted by a Dutch court of war crimes for both membership of a terrorist organization and degrading and humiliating treatment of dead bodies, as he had distributed a photo of himself in Syria via Facebook posing next to a deceased man hanging on a cross.[144] Between 2016 and 2018, Finland, Germany and Sweden prosecuted a series of similar cases of war crimes for 'outrages upon personal dignity', in particular humiliating and degrading treatment.[145]

Pathways to prosecution

To prosecute an international crime, it will be necessary both to identify the perpetrator and to gather evidence necessary to prove the elements of the crime. Where social media channels are used as a means of perpetrating or facilitating an international crime, various types of evidence may be useful. This includes mobile phone metadata such as upload times, usernames and log-in history;

143 Rome Statute, arts 8(2)(a)(ii) and 8(2)(c)(iii); see also p. 12 of this paper.
144 Lingsma, T. (2019), 'First Dutch Islamic State Fighter Convicted for War Crimes', JusticeInfo.Net, 25 July 2019, https://www.justiceinfo.net/en/42008-first-dutch-islamic-state-fighter-convicted-for-war-crimes.html.
145 For further discussion of these cases, see Eurojust (2018), 'Prosecuting War Crimes for Outrage Upon Personal Dignity', fact sheet, https://www.eurojust.europa.eu/publication/prosecuting-war-crimes-outrage-upon-personal-dignity-based-evidence-open-sources-legal. Under the Elements of Crime of outrages upon personal dignity, outrages can be perpetrated against unconscious persons, mentally handicapped persons or on dead bodies.

intercept/wiretap intelligence of communications between fighters; or open-source intelligence (OSINT). Examples of the latter include YouTube videos, Facebook posts, geospatial imagery or online forum comments.

Rules on the admissibility of evidence in court vary between jurisdictions. In civil law jurisdictions, for example, the inquisitorial system means that the court itself actively investigates and gathers evidence, including from the police. By contrast, in common law countries like Australia, Canada and the UK, where criminal law is tried by a judge and jury in an adversarial system, additional enquiries and further evidence (such as witness testimony) are typically needed to ensure that digital evidence is corroborated and therefore admissible. It is notable that the cases mentioned above were all prosecuted in civil law jurisdictions.[146]

Even where states have the jurisdictional basis in their domestic law to prosecute international crimes, many currently lack expertise, experience and resources in this area.

Even where states have the jurisdictional basis in their domestic law to prosecute international crimes, many currently lack expertise, experience and resources in this area. For those states that do have jurisdiction and resources, some war crimes units are still relatively new. International crimes units within prosecution authorities are typically detached from those that focus on cybercrime. But investigation and prosecution of cyber-enabled international crimes depend on expertise from both areas, so skills and communications should be pooled across teams. Development of this kind of pooled capability would help national authorities to take a proactive approach to identifying where cybercrimes may violate international criminal law as well as domestic criminal law.

In practice, cyber means will not usually be used in isolation to commit international crimes, but rather in combination with physical means. National authorities may choose to prosecute the cyber element as part of a wider package of criminal conduct. The paragraphs below discuss the diverse sources and types of evidence that may be relevant to cyber-enabled international crimes (and in some cases, to international crimes more broadly), as well as the frameworks available for prosecutors to obtain this evidence.

Frameworks for prosecutors to obtain evidence

In Scenario 1 above, it may be possible for state A to prove the identity of the perpetrator from the images on the smartphone. While the smartphone itself may be in state A's possession, access to the images and videos may be complicated if the fighter deleted them before being captured, or if they were stored on a server located outside the jurisdiction of state A. State A would also need to establish a lawful basis for accessing those images. In relation to the video's dissemination, state A would

146 Specifically, Finland, Germany, the Netherlands and Sweden.

need to establish how the images were distributed (for example, via which social media platform, to which audience, at what scale and with which effects). These issues would likely require cooperation between state A and other states and private actors (such as technology companies) to obtain the evidence required.

States typically cooperate with each other on the investigation or prosecution of criminal offences through mutual legal assistance. A mutual legal assistance treaty (MLAT) is an international agreement between states that facilitates cooperation on activities such as gathering evidence, locating suspects or freezing assets. Requests for assistance under bilateral MLATs are usually made through a formal letter to a central authority. However, MLAT procedures can be slow and bureaucratic, often taking months, if not years, to complete. A state receiving such requests for information may be reluctant to provide it, if it has concerns about due process or human rights in the requesting state (for example, if the requesting state enforces the death penalty for the offence in question). The receiving state may also be restricted in what it can provide under data protection law.[147]

The Ljubljana–The Hague Convention is the first international agreement specifically designed to facilitate mutual legal assistance in relation to the prosecution of *international* crimes.[148] The convention contains various provisions on exchange of evidence that are designed to bypass the bureaucracies of the MLAT system, including the spontaneous exchange of information relating to crimes and the establishment of single points of contact.[149] Once the convention enters into force, these provisions should speed up the exchange of evidence on international crimes between states parties.

Cybercrime treaties provide another route for states to obtain electronic evidence from another state, provided that the request for evidence is within the scope of the relevant treaty. As the OTP policy paper notes, certain conduct involved in cybercrime, such as the non-consensual hacking of a computer, may also form part of a cyber-enabled international crime.[150] Provisions on mutual legal assistance in recent cybercrime treaties are quite wide in scope – for example, the Budapest Convention on Cybercrime of 2001, which currently has 81 states parties (including the US),[151] refers to 'mutual legal assistance… for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data'.[152] Where there is no MLAT in place, the Budapest Convention could therefore provide a basis for states to make requests for evidence relating to cyber-enabled international crimes that concern computer systems and data. Such requests can be made on an expedited basis, if necessary, through a designated point of contact, available 24 hours a day, seven days a week.[153]

---

147 Force Hill, J. (2015), 'Problematic Alternatives: MLAT Reform for the Digital Age', *Harvard Law School National Security Journal*, 28 January 2015, https://journals.law.harvard.edu/nsj/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age.
148 See section 3.1 of this paper.
149 Government of Slovenia (2023), *The Ljubljana–The Hague Convention on International Cooperation in the Investigation and Prosecution of the Crime of Genocide, Crimes against Humanity, War Crimes and other International Crimes*, arts 17 and 21.
150 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 27.
151 See Budapest Convention.
152 Ibid., art. 25.
153 Ibid., arts 27, 26 and 35.

The UN Convention against Cybercrime, which was signed in Hanoi, Vietnam in October 2025 by 71 states and the EU, could be applied to cyber-enabled international crimes as well as ordinary cybercrimes, as it refers to general principles of cooperation in relation to 'the collecting, obtaining, preserving and sharing of evidence in electronic form of *any serious crime*'.[154] The UN convention, once in force, will require states parties to build their capacity to prosecute cyber-related crimes by criminalizing behaviour relevant to these crimes – for example, making access to a computer without permission an offence – and establishing single points of contact in relation to inter-state requests for evidence. In due course, the UN convention may attract support from a wider range of states than the Council of Europe's Budapest Convention, including those in the Global South.

The strengthening of procedures for exchanging electronic evidence under the UN Convention against Cybercrime could therefore be useful in the context of prosecution of cyber-enabled international crimes. At the same time, civil society groups continue to raise concerns about inadequate human rights safeguards in the UN convention, especially in terms of cooperation between States.[155] Once the UN convention comes into force, it will be important that states parties implement their obligations in accordance with international human rights law.

Some states may seek to access data in the territory of other states without consent for the purpose of investigating cybercrime or cyber-enabled international crimes (for instance, by covertly gaining access to networks in another state) because relevant data is increasingly stored beyond national borders. Where evidence of a cyber-enabled international crime has been obtained in this way, several issues arise. Firstly, some states and scholars consider that obtaining information in this way could constitute a violation of international law.[156] If so, the question arises as to whether a court would admit the evidence in court. Even if it did – for which there is some precedent[157] – a state may be reluctant to submit the evidence to court because they may not wish to reveal how it was obtained. As the national position of the Netherlands notes, opinion is divided as to what qualifies as exercising investigative powers in a cross-border context and, 'the manner in which the principle of sovereignty should be applied has not fully crystallised at the international level'.[158]

---

154 UN Convention against Cybercrime, art. 35 (emphasis added).
155 Brown, D. (2024), 'New UN Cybercrime Treaty Primed for Abuse', Human Rights Watch, 30 December 2024, https://www.hrw.org/news/2024/12/30/new-un-cybercrime-treaty-primed-abuse.
156 See, for example, para 15 of the Common Position of the African Union on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace, 29 January 2024; Heller, K. J. (2024), 'The African Union (Rightly) Endorses Pure Sovereignty in Cyberspace', Opinio Juris, 5 February 2024, https://opiniojuris.org/2024/02/05/the-african-union-rightly-endorses-pure-sovereignty-in-cyberspace.
157 For example, in the *Corfu Channel* case (UK v Albania) ICJ Reports p. 4, the ICJ admitted evidence that had been illegally obtained by the UK. See Fallah, S. (2022), 'Illegally Obtained Evidence: International Adjudication' in the Max Planck Encyclopaedia of International Law.
158 Government of the Kindgom of the Netherlands, Appendix: International law in cyberspace, 26 September 2019.

Obtaining open-source digital data

In the cases prosecuted in Germany, Finland and Sweden, publicly available, electronically recorded footage of the crimes charged and online commentary by the defendants about the crimes charged were crucial to the success of the prosecutors' case.[159] Increasingly, NGOs and 'citizen journalists' also gather their own information to support accountability for international crimes.[160]

As with more traditional types of evidence, a court would need to look carefully at the credibility of open-source digital information, including the clarity of the information presented and the nature of the organization presenting it.[161] Where open-source evidence is in digital format, manipulation is easy to do and often hard to detect.[162] AI tools can be used to fabricate audio recordings and digital evidence (e.g. through deepfakes) to a convincing standard, potentially undermining the credibility of video footage presented in legal proceedings and jeopardizing prosecution.

Owing to the potential for manipulation, in the scenario above, it would be necessary first to authenticate the video in the proceedings.

The difficulty sometimes of proving the provenance and reliability of open-source material means that prosecutors will often seek to corroborate digital materials with other forms of evidence such as witness testimony or intelligence reports. In the case of *Bemba et al*, the prosecution's submission of photos posted on Facebook was challenged by the defence on the grounds that the images had not been properly verified. In that case, however, the Trial Chamber held that the facts had been adequately established through alternative evidence.[163]

Another potential problem in this context is that social media companies sometimes take down content that could constitute valuable evidence where their algorithms detect a violation of terms of service.[164] Often, these removals occur precisely because the content is deemed violent or inhumane. But when digital platforms remove content, nothing generally prevents them from preserving that content and any other relevant data for future investigations. Where there is a serious risk of international crimes being committed, platforms should preserve evidence on their own initiative.[165]

---

159 Secretariat of the Genocide Network (2018), *Prosecuting war crimes of outrage upon personal dignity based on evidence from open sources – Legal framework and recent developments in the Member States of the European Union*, report, The Hague: Eurojust, https://www.eurojust.europa.eu/publication/prosecuting-war-crimes-outrage-upon-personal-dignity-based-evidence-open-sources-legal.
160 For example, Pigott, P. (2022), 'Ukraine: Online posts transform war crimes documentation', BBC News, 17 April 2022, https://www.bbc.co.uk/news/uk-wales-61011855. Organizations such as Bellingcat and University of California, Berkeley also conduct investigations into potential international crimes using the latest technology, including satellite imagery and geolocation, and make their findings available to any national or international prosecutors who are gathering evidence of such crimes.
161 *Prosecutor v Jean-Pierre Bemba Gombo* (ICC-01/05-01/08 (27 June 2013), para 269.
162 Freeman, L. (2021), 'Weapons of War, Tools of Justice: Using Artificial Intelligence to Investigate International Crimes', *Journal of International Criminal Justice*, 19(1), pp. 35–53, https://doi.org/10.1093/jicj/mqab013, p. 47.
163 Defence Response to Prosecution's Third Request for the Admission of Evidence from the Bar Table, *Prosecution v Bemba et al* (ICC-01/05-01/13), Trial Chamber, 9 October 2015, paras 83–86.
164 Goodman, J. and Korenyuk, M. (2023), 'AI: war crimes evidence erased by social media platforms', BBC News, 1 June 2023, https://www.bbc.co.uk/news/technology-65755517.
165 See also ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, p. 150, which notes that the OTP will work with relevant stakeholders to explore the desirability of clear guidelines for cooperation on data preservation requests.

Non-public content and non-content data

National prosecuting authorities may need information from technology companies that is not available publicly – for example, private messages sent via social media or IP history from internet platforms. The relevant evidence will often be held by one of the large US-based technology companies that dominate the market for such services (e.g. Google, Meta, Microsoft and X). However, US law prohibits technology companies in the US from being able to share certain data in response to requests from foreign governments. The Stored Communications Act (SCA) in particular contains restrictions on companies disclosing the contents of stored electronic communications,[166] while the Electronic Communications Privacy Act 1986 (ECPA) restricts telecommunications companies from the disclosure of certain content data such as email.[167]

Private entities may also be subject to conflicting obligations in relation to the handling of data – for example, when a company receives an order from a government in one state requiring the disclosure of data, but due to the policies of the company (e.g. on user privacy) or laws of the host state, the company is not in a position to hand over the data requested. For example, Telegram is well known for taking a strong stance on user privacy. In the context of accusations against it of enabling cybercriminals,[168] the company changed its policy to enable the provision of some user data to law enforcement authorities, including for cybercrime investigations.[169] Commercial and prosecutorial interests may also conflict: if, for instance, a private company providing technical assistance to a prosecuting authority in relation to one matter is implicated in one of the situations that the authority is deciding whether to investigate.

In recent years, states have developed avenues to facilitate access to information from US technology companies. The US Clarifying Lawful Overseas Use of Data Act (Cloud Act), enacted in 2018, amended the SCA to require US telecommunications companies to provide data in their possession, and to enable foreign governments to seek data directly from those companies without prior review by the US government. So far, the US has entered into bilateral agreements with two countries: Australia and the UK. The UK–US Data Access Agreement allows US and UK law enforcement agencies directly to request data held by the telecommunications providers in the other party's jurisdiction, for the exclusive purpose of preventing, detecting, investigating and prosecuting serious crimes such as terrorism or child sexual abuse and exploitation.[170] The agreement covers subscriber information, as well as content data.

---

166 Stored Communications Act (SCA), s.2701(a)(i).
167 The Electronic Communications Privacy Act 1986 (ECPA), 18 U.S.C. §§ 2510-2523.
168 Tidy, J. (2024), 'Telegram: 'The dark web in your pocket'', BBC News, 31 August 2024, https://www.bbc.co.uk/news/articles/cdey4prn3e1o.
169 Toulas, B. (2025), 'Telegram hands over data on thousands of users to US law enforcement', Bleeping Computer, 7 January 2025, https://www.bleepingcomputer.com/news/legal/telegram-hands-over-data-on-thousands-of-users-to-us-law-enforcement.
170 The UK–US Data Access Agreement, which was enacted under the US Cloud Act 2018, came into force on 3 October 2022. See Home Office (2022), *UK-US Data Access Agreement*, policy paper, https://www.gov.uk/government/publications/uk-us-data-access-agreement-factsheet.

Another route for prosecutors to gather evidence from US technology companies is through subsidiaries of those companies based elsewhere in the world, where applicable. For example, most of the major US-based technology companies have subsidiary offices in Ireland. States wishing to obtain data from those companies may be able to submit a request to the relevant authorities in Ireland (rather than to their US headquarters), which could then obtain a court order to compel the Irish subsidiary company to provide the requested information. In assessing a request, companies take into account not only Irish law (which does not contain the same restrictions on sharing content data as the US ECPA), EU law (including data protection law such as GDPR), the law of the requesting country (including compliance with the rule of law), international norms (including international human rights law), and the company's own policies.[171]

Some technology companies have become more comfortable with responding to government requests for non-content data on a voluntary basis, subject to consideration of legal and policy issues.

The US ECPA only applies to content data. Some technology companies have become more comfortable with responding to government requests for non-content data – such as registration data, IP history and device information – on a voluntary basis, subject to consideration of the legal and policy issues above.[172] When a technology company is assessing whether the requesting state complies with the rule of law, it will take into account whether that state is a party to the Budapest Convention, which requires states parties to abide by certain human rights safeguards in relation to the handling of information by law enforcement authorities.

Under the EU's e-Evidence Framework, which is due to take effect from 2026, law enforcement and judicial authorities in one member state will be able to request electronic evidence, including subscriber data, directly from a service provider in another member state.[173] The EU's e-Evidence Regulation requires a broad range of service providers (including internet domain name entities, internet service providers and cloud service providers) to preserve certain data categories on receipt of an order,[174] and to disclose them within 10 days

171 See, for example, Google's policies on law enforcement requests: Google (undated), 'How Google handles government requests for user information', https://policies.google.com/terms/information-requests?hl=en-US.
172 Daskal, J. (2016), 'Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues', *Journal of National Security Law and Policy*, 8(3), https://nationalsecurity.law.georgetown.edu/journal/2016/09/06/law-enforcement-access-data-across-borders-evolving-security-rights-issues.
173 The framework consists of an e-Evidence regulation and directive, both of which will establish unified European rules for the preservation and disclosure of electronic evidence in relation to any offence. See Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, which will apply from 18 August 2026 and Directive (EU) 2023/1544 laying down harmonized rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings, which EU member states must transpose into national law by 18 February 2026.
174 Under the terms of EU e-Preservation Orders (para 60 of the regulation), service providers are obliged to preserve data for 60 days, with a possible extension of 30 days.

of receipt of an EU e-Production order. The Second Additional Protocol to the Budapest Convention will also enable states parties to obtain electronic data (such as subscriber information and traffic data) directly from service providers located in other countries, regardless of whether there is an MLAT in place.[175] While the protocol is not yet in force, some of the major technology companies are already working to ensure compliance with its provisions as a matter of policy.

These rules are an improvement on the current situation, in which prosecutors must deal with a variety of company policies on disclosure and preservation of evidence. Further, those companies that either do not have a well-established preservation policy or have been refusing to comply with requests for disclosure will now have to comply. SIRIUS, an EU-funded project, helps law enforcement and judicial authorities in EU member states to access cross-border electronic evidence in the context of criminal investigations and proceedings.[176] It has 8,000 members from the law enforcement and judicial communities, representing 47 countries worldwide, and has directly supported 70 police operations.[177]

However, even when technology companies do hand over information requested by law enforcement agencies, those agencies may lack the capacity to deal with the volume of data provided, both in terms of storage and authentication. Some states, such as France, the Netherlands, Singapore, the UK and the US, have implemented digital evidence management systems (DEMS) that facilitate the storage, indexing and analysis of digital evidence.[178] But many other states lack these resources.

National prosecuting authorities investigating international crimes may also seek support from the OTP.[179] The OTP's policy paper on cyber-enabled international crimes notes that such support may include intelligence-sharing, evidence, situation briefs, and holding strategic consultations on case selection and prioritization.[180] Cooperation between states and the OTP is discussed in more detail in the scenarios below.

---

175 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CETS No. 224, open for signature 12 May 2022, art. 7.
176 SIRIUS is co-funded by Europol and Eurojust, in close partnership with the European Judicial Network. The project provides products such as standardized guidelines on cooperation processes between competent authorities and service providers; investigation tools; contact details for service providers; and a restricted platform for sharing knowledge and best practice. See Europol (2025), 'SIRIUS project' (updated 13 Nov. 2025), https://www.europol.europa.eu/operations-services-innovation/sirius-project.
177 European Commission (2025), 'Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and Committee of the Regions: Roadmap for lawful and effective access to data for law enforcement' COM (2025) 349 final, 24 June 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0349.
178 For example, the Dutch government and those of several other countries use an open digital forensic platform called Hansken for criminal justice. See European Institute of Public Administration (undated), 'Hansken, the open digital forensic platform', https://www.eipa.eu/epsa/hansken-the-open-digital-forensic-platform.
179 Rome Statute, art. 93(10).
180 Ibid., para 142.

4.2 Investigation and prosecution by the ICC

Scenario 2

In an armed conflict taking place in state A (a party to the Rome Statute), a commander of state A uses AI-powered facial recognition and surveillance systems to identify and track hundreds of journalists and human rights defenders. The commander then uses an encrypted online messaging platform to order his troops to target and kill those civilians, in violation of international humanitarian law. Neither state A nor other states are willing or able to prosecute the commander.

This section analyses pathways available to the OTP to investigate and prosecute cyber-enabled international crimes.[181]

Pathways to prosecution

In Scenario 2, since the alleged crimes take place on the territory of a state party, the ICC will have jurisdiction.[182] Unlike national prosecutors, the OTP does not have law enforcement powers itself (so cannot, for example, issue subpoenas for evidence or search warrants). And, unlike states, the OTP does not have agencies that regularly gather intelligence. Therefore, if the OTP decides to open an investigation into the facilitation or perpetration of an international crime by cyber means, cooperation with states, intergovernmental organizations, the private sector and civil society to help identify those responsible and gather the evidence necessary to prosecute them will be crucial.

In cooperating with any external party, the OTP needs to maintain the independence and impartiality of the prosecutor.[183] There can be, for example, a risk of conflict of interest where businesses that cooperate with the court are potentially implicated in some of the ICC's work – for example, if information supplied by technology companies is relevant to the OTP's investigation of a situation in which technology companies themselves are implicated because they supply IT services to militaries in an armed conflict that is part of the OTP's investigation.

As the OTP policy paper notes, technical digital evidence may be of particular importance in establishing how cyber-enabled international crimes were committed and in attributing conduct to perpetrators.[184] The Rome Statute does not place any restrictions on the types of evidence that may be admissible before the ICC. The ICC's assessment of the weight given to evidence is also flexible.[185] The ICC has experience in dealing with digital evidence, including videos and social media posts. For example, in the 2016 case concerning Malian Islamist

181 If an individual uses AI to commit a crime, criminal responsibility will arise, just as with the use of any other tool.
182 See p. 34 of this paper.
183 As the OTP affirms in its policy paper. See ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 128.
184 Ibid. para 161.
185 *Bemba*, Judgment pursuant to article 74 of the Statute, Trial Chamber III, 21 March 2016, ICC-01/05'01/08-3343, para 235; *Lubanga* Trial Judgment, para 107.

militia member Ahmad al-Faqih Al Mahdi, videos from YouTube helped to secure a conviction for the war crime of destruction of cultural property.[186] Another example is an arrest warrant issued by the ICC for Libyan commander Mahmoud Mustafa Busayf al-Werfalli in 2017, which relied on a wide range of open-source evidence including social media posts featuring executions,[187] alongside witness interviews and reports from international organizations, NGOs and research centres. Evidence from Facebook was touched on briefly, although not ultimately relied upon, in the cases of *Yekatom and Ngaissona* and *Abd-Al-Rahman*.[188]

Technical digital evidence may be of particular importance in establishing how cyber-enabled international crimes were committed and in attributing conduct to perpetrators.

The ICC has systems in place to store, manage and review the digital evidence that will inevitably form part of a case with a cyber element. This includes a cloud-based, centralized data storage system (OTP eVault), an evidence review and analysis platform featuring generative AI tools with a particular focus on legal data (OTP eDiscovery),[189] and an e-court protocol to help streamline the process for using digital evidence before the court. Since 2023, the OTP has also been able to collect digital materials (such as user-generated content from smartphones) directly through a dedicated online platform, OTP Link. This platform enables users – including victims, witnesses, civil society organizations and governmental bodies – to upload files (up to 1,000 per submission) for the purpose of preserving content for future proceedings.

Cooperation between the OTP and states

In Scenario 2, it is likely that the OTP would need to seek information from state A and any other states that may have relevant information, including from intelligence sources. Even if the states concerned are not party to the Rome Statute, or are not otherwise prepared to cooperate with the OTP, other state parties may be able to help.

Part 9 of the Rome Statute sets out arrangements for international cooperation and judicial assistance. States parties are obliged to cooperate with the ICC and to make procedures available under national law for all forms of cooperation.[190] Forms

---

186 *The Prosecutor v Ahmad Al Faqi Al Mahdi*, ICC-01/12-01/15.
187 *The Prosecutor v Al-Werfalli*, ICC-01/11-01/17.
188 See McDermott Rees, Y., Hausnecht, A. and Liefgreen, A. (2025), 'New Evidence, New Challenges: ICC Judges' Perspectives on User-Generated Evidence and Judging in an Age of Artificial Intelligence', *Onati Social-Legal Series*, 16(1), https://cronfa.swan.ac.uk/Record/cronfa71069, p. 2; *The Prosecutor v. Alfred Yekatom and Patrice-Edouard Ngaïssona*, Trial Judgment, ICC-01/14-01/18-2784 (24 July 2025); *The Prosecutor v. Ali Muhammad Ali Abd-Al-Rahman* ('Ali Kushayb'), Trial Judgment, ICC-02/05-01/20-1240 (6 October 2025).
189 Features include rapid pattern identification, automatic translations, facial identification, image enrichment, translations of media files, targeted searches of source material, and video and image analytics. See Evans, H. and Hazim, M. (2023), 'Digital Evidence Collection at the International Criminal Court: Promises and Pitfalls', Just Security, 5 July 2023, https://www.justsecurity.org/87149/digital-evidence-collection-at-the-intl-criminal-court-promises-and-pitfalls.
190 Rome Statute, arts 86 and 88.

of cooperation include the taking of evidence, service of documents, execution of searches and seizures, and provision of records and documents.[191] States can assist the OTP not only in providing evidence themselves but also in issuing compulsory orders to companies, individuals or others to give that evidence to the state, which can then pass it to the OTP.[192] The OTP may seek the assistance of states in identifying, tracing and freezing the means used to carry out cyber-enabled crimes[193] – for example, in Scenario 2, by asking state A for information about the use of the surveillance system.

Like the MLAT system, the Part 9 system can be bureaucratic and time-consuming. For example, if the OTP wishes to obtain data from a private company based in a state party through formal channels, the OTP will need to make a request through the channel designated by that state (such as the foreign ministry or justice ministry),[194] which will pass it on to the relevant department(s) or agencies, which in turn may then need to obtain a court order to seek the information in question. Another challenge is that, although there are procedures in place for states to provide the OTP with confidential information, states parties have the right to deny a request for assistance on national security grounds.[195] The OTP has been working to streamline the Part 9 system so that cooperation with states is more efficient and, where appropriate, to make additional arrangements. In its policy paper, the OTP notes the importance of deepening engagement with national authorities.[196]

As noted in Scenario 1, the EU's e-Evidence package and the Second Additional Protocol to the Budapest Convention, once in force, have more efficient procedures. Where states parties to the Rome Statute are also parties to these instruments, the OTP might be able to ask those states to issue direct requests to companies (in the case of the EU, through a European Production Order) and then to pass on the information they have received from them. Currently, all EU member states are states parties to the Rome Statute, as well as being represented in both Europol and Eurojust.[197] Therefore, when the OTP requests assistance from EU states (either in relation to digital evidence that they hold or that is held by companies within their jurisdiction), those states may be able to draw on relevant powers and resources from these EU-based organizations.

The OTP has strengthened its relationships with each of these organizations in recent years, which is likely to facilitate its investigation and prosecution of cyber-enabled international crimes. In 2022, Eurojust's regulation was amended to allow Eurojust to make evidence directly available to the ICC.[198] In September 2024, the ICC signed a working arrangement with Europol to enhance cooperation and the exchange

191 Rome Statute, art. 93.
192 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 162.
193 Ibid., para 178.
194 Rome Statute, art. 87.
195 Rome Statute, arts 72 and 73.
196 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 133.
197 On 2 June 2025, Hungary notified the UN secretary-general of its withdrawal from the Rome Statute. The withdrawal will take effect on 2 June 2026.
198 Amending Regulation (EU) 2022/838 of 30 May 2022 as regards the storage, preservation and analysis of evidence in war crimes, which came into force on 1 June 2022.

of information and expertise.[199] At the same time, the ICC signed a memorandum of understanding with Europol to allow access to the latter's SIENA network, a platform that enables swift exchange of operational and strategic crime-related information among Europol's liaison officers, analysts and experts, member states, and third parties with which Europol has cooperation agreements, including states outside the EU such as Australia, Canada and the US.[200] In December 2024, the OTP entered into a cooperation agreement with Interpol, under which the parties can exchange information, and the OTP can access Interpol's I-24/7 network and database system, which facilitates rapid and secure data-exchange between law enforcement contact points around the world.[201]

The OTP may also ask states to cooperate on a voluntary basis.[202] In 2024, the ICC launched a Policy on Complementarity and Cooperation, including a forum that serves as a platform for the two-way sharing of information and expertise between the OTP and national authorities.[203] This forum might be helpful, for example, in relation to requests to states to preserve evidence of cyber-enabled international crimes, pending the opening of a full investigation.[204] As well as having the authority to request states parties for cooperation, the court can also make ad hoc arrangements with non-state parties.[205]

The ICC is not itself a party to cybercrime treaties such as the Budapest Convention. But, as the OTP policy paper suggests, 'there may be mutual value in pooling [with national authorities] capabilities, techniques, skills, and procedures related to the investigation of conduct in cyberspace'.[206] For the purpose of investigations and prosecutions under the Rome Statute, the OTP intends to seek the support of states parties and any other interested states to conclude voluntary agreements extending similar assistance to the OTP as is available for states under new treaties such as the Second Additional Protocol to the Budapest Convention and the UN Convention against Cybercrime.[207]

As noted in Scenario 1, recently adopted treaties on cybercrime will require states to build up their techniques and procedures in relation to the preserving and sharing of digital evidence, which is likely to equip states better to handle requests from the OTP for digital evidence.

---

199 Europol (2024), 'ICC and Europol sign Liaison Officer Agreement and SIENA Memorandum of Understanding', press release, 18 September 2024, https://www.europol.europa.eu/media-press/newsroom/news/icc-and-europol-sign-liaison-officer-agreement-and-siena-memorandum-of-understanding.
200 Ibid.
201 ICC (2004), 'Cooperation agreement between the Office of the Prosecutor and Interpol', press release, 22 December 2004, https://www.icc-cpi.int/news/icc-cooperation-agreement-between-office-prosecutor-and-interpol.
202 The OTP's policy paper on cyber-enabled international crimes references (at fn 175) *Situation in Burundi*, in which the court noted that the prosecutor may seek voluntary cooperation from states parties.
203 ICC Office of the Prosecutor (2024), *Policy on Complementarity and Cooperation*, https://www.icc-cpi.int/sites/default/files/2024-04/2024-comp-policy-eng.pdf.
204 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 150.
205 Rome Statute, art. 87(5)(a).
206 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 27.
207 Ibid., para 187.

Cooperation with private actors

In Scenario 2, the OTP would also need to seek information from the companies that make the AI-powered facial recognition and surveillance systems, and the company hosting the encrypted messaging platform. OTP cooperation with private actors will often be vital in the prosecution of cyber-enabled international crimes, especially where private companies own the cyber infrastructure used to commit those crimes. However, as has been noted, there is a tension between technology companies' cooperation in investigations into international crimes and the risk of those companies becoming complicit in the commission of such crimes – for example, through the provision of IT services to armed forces.[208] In dealing with private companies, it is important that the OTP manages these risks carefully and keeps them under regular review, including by ensuring that OTP staff are aware of the risk of conflicts of interest and the importance of impartiality and confidentiality.

OTP cooperation with private actors will often by vital in the prosecution of cyber-enabled international crimes, especially where private companies own the technical infrastructure used to commit those crimes.

There are various routes by which the OTP can access evidence from private companies. As noted above, the OTP can request a state party to obtain data from a company based in that state's jurisdiction. Where the information needed is held by a US company that has a subsidiary in Dublin, the OTP may be able to ask law enforcement authorities in Ireland (as a state party to the Rome Statute) to seek a court order to compel the company concerned to provide the information.

Data localization laws may offer the OTP alternative access points to US-controlled data. In some states parties, such as Nigeria, information held by private companies must be stored within that state's jurisdiction or, at least, be made accessible for law enforcement purposes.[209] In countries with such laws in place, the OTP could request the state party to compel the company to provide the information under relevant data localization laws. Companies will likely refuse to comply if they consider a request to be incompatible with their terms of service. But some states have

---

208 Claims have been reported regarding the alleged complicity of some technology companies in international crimes during Israel's conflict with Gaza. See, for example, Business and Human Rights Resource Centre (2025), 'Big Tech companies face allegations of war crimes complicity amid Israel's war in Gaza', 2 April 2025, https://www.business-humanrights.org/en/latest-news/big-tech-companies-allegedly-complicit-in-war-crimes-amid-israels-war-in-gaza-incl-company-responses. In August 2025, Microsoft announced a formal review of allegations reported by the *Guardian* that its Azure cloud platform has been used by a unit of the Israeli Defence Forces to store the data of phone calls obtained through broad or mass surveillance of civilians in Gaza and the West Bank. Microsoft provided an update on that review in September 2025. See Microsoft (2025), 'Update on ongoing Microsoft review', 25 September 2025, https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review. Also in September 2025, Microsoft terminated the Israeli military's access to some of its technology after accusations of usage that violated Microsoft's terms of service. See Davies, H. and Abraham, Y. (2025), 'Microsoft blocks Israel's use of its technology in mass surveillance of Palestinians', *Guardian*, 25 September 2025, https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians.

209 See Techpoint.africa (2025), 'NITDA's new rule mandates cloud providers to host key data within Nigeria', 12 February 2025, https://techpoint.africa/news/nitda-cloud-providers-host-data.

powers under their domestic law to compel data sharing in certain circumstances, for example, in order to fulfil a legal obligation in the context of a criminal investigation, or following a judicial order.[210]

In addition to compulsory requests, the OTP may request information from companies on a voluntary basis, within the framework of their applicable legal obligations.[211] In recent years, the OTP has built connections with cybersecurity firms and global service providers, which could provide a basis for broader voluntary sharing of information. There is precedent for direct sharing of evidence between social media companies and the ICC, although this practice varies across platforms. As well as holding data, platforms carry out their own investigations in some cases, which may also yield information useful for investigators. In general, however, companies prefer compulsory requests compelling the disclosure of the contents of an account, because such requests provide a clear legal framework for the company to follow and avoid setting a precedent in relation to cooperation.

US sanctions imposed on the ICC prosecutor and certain judges by the administration of President Donald Trump in 2025 place 'US persons' at risk of penalties if they support the court's work. While these sanctions are the subject of litigation in the US courts,[212] they are likely to make US companies cautious about cooperating with the court on investigations.

Cooperation with civil society

The OTP recently established an enhanced structural dialogue with civil society organizations, committing to hold two thematic roundtable discussions a year.[213] As part of this, the OTP has met with civil society organizations to discuss cyber-enabled international crimes. In the policy paper, the OTP underlines its commitment to working with civil society organizations in this area.[214] The policy also refers multiple times to international human rights law, underlining its importance as an adjacent framework in the context of cyber-enabled international crimes. For example, international human rights law provides standards on hate speech, which may be relevant to the consideration of online incitement to genocide. The policy also sets out the OTP's commitment to work with civil society and the private sector to enhance and clarify voluntary frameworks for the sharing of information and expertise with the court.[215]

---

210 For example, Brazil, under its General Data Protection Law, No. 13.709/2018.
211 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 162.
212 See Milaninia, N. (2025), 'Legal Challenges Mount Against Renewed U.S. Sanctions Against the ICC', Lawfare, 9 May 2025, https://www.lawfaremedia.org/article/legal-challenges-mount-against-renewed-u.s.-sanctions-on-the-icc.
213 ICC Office of the Prosecutor (2024), *Policy on Cooperation and Complementarity*, paras 43 and 83.
214 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 192.
215 Ibid., para 194.

4.3 The multi-agency approach: Coordinated investigation and prosecution by states, with OTP support

Scenario 3

A high-profile criminal group based in state A, and supportive of the agenda of state A, launches a simultaneous widespread ransomware operation on the healthcare systems of states B and C. The operation cripples the healthcare services of states B and C nationwide for weeks. As a result, states B and C declare a state of emergency, hundreds of patients die and the health of hundreds of thousands is affected. The members of the criminal group are accused of crimes against humanity.

In 2021, a criminal gang believed to be operating from Russia, known as the Conti group, launched a ransomware operation on Ireland's healthcare system that resulted in significant disruption to healthcare systems across the country for months.[216] In 2022, a ransomware operation against Costa Rica resulted in a 'state of emergency' being declared after multiple government institutions – including the finance ministry – had their essential services disrupted for weeks.

Scenario 3 looks at a situation in which states B and C form a joint investigation team, supported by Eurojust, Europol, Interpol and the ICC. In doing so, the scenario explores a growing trend for coordinated approaches to the pursuit of accountability for international crimes. Joint investigations allow two or more investigative, prosecutorial or judicial bodies to coordinate in respect of common lines of inquiry, or work alongside each other in specific operations.[217] In its policy paper, the OTP proposes, where appropriate, to work collaboratively with states to investigate cyber-enabled crimes under the Rome Statute and disrupt such activities where they may be ongoing.[218] The OTP also notes its intention to expand its participation, where appropriate, in joint investigations.[219] Various new treaties provide procedures to facilitate such investigations.[220]

The complexity of cyber investigations

The investigation and prosecution of cyber operations such as ransomware can be highly complex, whether those operations are conducted by states, criminal gangs or both acting together.

---

216 A ransomware attack is a malware attack that prevents the user from accessing the device or the data on it. For details on the Conti group incident, see Health Service Executive (2021), *Conti Cyber Attack on the HSE: Independent Post Incident Review*, report, 3 December 2021,https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf.
217 ICC Office of the Prosecutor (2024), *Policy on Cooperation and Complementarity*, para 102.
218 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 135.
219 Ibid., para 150.
220 For example, see Government of Slovenia (2023), *The Ljubljana–The Hague Convention on International Cooperation in the Investigation and Prosecution of the Crime of Genocide, Crimes against Humanity, War Crimes and other International Crimes*, art. 41; the Second Additional Protocol to the Budapest Convention, art. 12; and the UN Convention against Cybercrime, art. 48.

First, it is necessary to identify the digital infrastructure, network or device used to carry out the operation, which will likely involve the expertise of software engineers to track and trace digital evidence such as log files.

Second, it is necessary to identify who was responsible for the operation. States and the technology industry have made significant progress in the technical attribution of cyber operations to states or groups.[221] However, when a state is involved in the crime, that crime must be attributed to an *individual* to enable prosecution.

Finally, even then, establishing that a particular individual owned the device used to launch the attack is not enough on its own. Further evidence will be needed to connect that individual to the cyber activity concerned. Malicious actors will often seek to cover their tracks, by using proxies (an intermediary server that masks the user's IP address) or virtual private networks. Evidence such as device fingerprints, browser history or intercept intelligence may help to prove the involvement of an individual. The investigation is likely to require real-time coordination of intelligence and the securing of evidence from states and private sector providers across multiple jurisdictions.

Few states have the resources to undertake complex prosecutions alone, not least because such prosecutions are expensive.

Few states have the resources to undertake these complex prosecutions alone, not least because such prosecutions are expensive. Over the last 10 years, the US has issued indictments against Chinese, Iranian, North Korean and Russian actors for the use of destructive malware through unauthorised access to computers. However, the US is unusual in having highly skilled cross-government units able to investigate and prosecute cybercrime, as well having many of the major technology companies located within its jurisdiction, which facilitates access to evidence. The US also required the help of other actors to bring some of the cases mentioned above. For example, the US indictment of Russian GRU officers for hacking Ukrainian government networks and probing NATO member states involved an international effort including the FBI and 12 other partners, representing governments of nine countries, as part of 'Operation Toy Soldier'.[222]

A multi-agency approach – involving states, cybersecurity companies, international organizations such as Eurojust, Europol and Interpol, as well as potentially cooperation with the ICC – can facilitate the investigation and prosecution of an international crime that involves a major cyber operation. This section therefore focuses on a situation in which states and other actors work together to investigate and prosecute a major cyber operation that, in addition to being a cybercrime, also constitutes a cyber-enabled international crime. This scenario is topical – in the

221 Schöndorf notes that '[o]ver time, the attribution capabilities of States have improved, and even States with lesser capabilities have been able to rely on solid information provided by other States and by the private sector'. See Schöndorf (2021), 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations', p. 404.
222 *US v Stigal, Borovkov, Denisenko, Denisov, Goloshubov and Korchagin* at footnote 123.

area of ransomware, states' use of 'proxy' relationships (i.e. cooperation with non-state actors, such as hackers and criminal groups) to carry out cyberattacks is increasing,[223] including by Russia in the context of its war on Ukraine.[224]

In Scenario 3, investigators and prosecutors of the cyber-enabled international crime will be seeking similar types of evidence, and using similar frameworks, to those used in the investigation and prosecution of cybercrime. Lessons can therefore be drawn from the increasingly collaborative approaches used to tackle cybercrime.

Public–private partnerships

In investigating a ransomware attack, close cooperation with the private sector is vital. As in the previous scenarios, cloud providers may not only hold important digital evidence, they may also be able to assist with technical information (such as network traffic reports) that provide insights into the activities of hacker groups. Cybersecurity companies can provide cyberthreat intelligence and digital forensic analysis, which can help identify details such as the type of digital infrastructure or device used for an operation, the identity of the perpetrator, and the tactics, techniques and procedures used by the perpetrator. The combination of private sector detection technology and state intelligence can be highly effective.

Public–private cooperation in relation to the prosecution of cybercrime is growing. Microsoft, for example, has a well-established Digital Crimes Unit, operates a Threat Analysis Center, and provides reports on malicious cyber activities.[225] Like Microsoft, cybersecurity firms such as CrowdStrike, Mandiant (part of Google Cloud) and Trellix (formerly FireEye), which specialize in threat intelligence and detection, have helped governments to trace chains of proxy servers, and to expose and respond to harmful cyber operations.[226] Some governments have formed public–private task forces to assist with identification of harmful cyber activity. For example, the US Cybersecurity and Infrastructure Security Agency set up the Joint Cyber Defense Collaborative, which brings together firms like CrowdStrike, Mandiant, Microsoft and Palo Alto Networks. Some governments also contract with private companies on attribution efforts and forensic investigations.[227]

The majority of private sector cyber intelligence is based in the US and subject to US jurisdiction. As noted above, the strained relationship between the US and the ICC – particularly recent US sanctions against the prosecutor and certain judges – may dampen the prospects of cooperation by US companies on the investigation and prosecution of international crimes.

---

223 Milenkoski, A. et al. (2025), *Ransomware's New Masters: How States are Hijacking Cybercrime*, report, Virtual Routes, https://virtual-routes.org/wp-content/uploads/2025/04/Virtual-Routes-Pharos-Report-Series-No.-3.pdf.
224 Huntley, S. (2023), 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape', Google Threat Analysis Group, 16 February 2023, https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape.
225 For example, Microsoft's reports on the latest threats in Ukraine have included details of Russian cyber operations targeting the criminal investigators and prosecutors who are building cases against them for war crimes. See Watts, C. (2023), 'Russian influence and cyber operations adapt for long haul and exploit war fatigue', blog post, Microsoft On The Issues, 7 December 2023, https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac.
226 For example, FireEye uncovered the major SolarWinds supply-chain cyberattack. See National Cyber Security Centre (2021), 'NSCS Annual Review 2021', report, London: NCSC, https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/solarwinds, p. 10.
227 For example, PWC investigated and prepared a detailed report on the Conti cyber ransomware attack on the Irish health service in 2021. See Health Service Executive (2021), *Conti cyber attack on the HSE*.

However, some technology companies, including US companies, have been strengthening cooperation with law enforcement agencies on cybercrime, which may also have benefits for the investigation and prosecution of cyber-enabled international crimes. For example, the EU's Agency for Cybersecurity (ENISA) engages with private sector actors on threat intelligence and attribution, while Europol and Interpol also have formal partnerships with private companies in the cybersecurity and information technology industries.[228]

Over 140 states have established computer incident response teams, which use the latest developments in technology to help trace the origins of cyber operations, identify perpetrators and link attacks across borders.

Over 140 states have established computer incident response teams (CIRTs), which use the latest developments in technology to help trace the origins of cyber operations, identify perpetrators and link attacks across borders.[229] Cooperation between CIRTs is growing through regional CIRT–CIRT arrangements for the exchange of information about harmful cyber operations. A UN Points of Contact Directory, established in 2024, should help to reinforce these arrangements.[230] Cybersecurity firms and CIRTs may be useful as advisers or even expert witnesses in cases involving cyber-enabled international crimes. At the same time, care is needed when states and international tribunals are dependent on private companies for evidence that, in the physical world, would have traditionally come from state intelligence agencies.

Civil society organizations can also help states with investigations into harmful cyber operations. For example, MITRE Corporation, a US not-for-profit, has created a globally accessible, knowledge-based framework of adversary tactics and techniques,[231] which is used by the UK's National Cyber Security Centre and others to help with attribution.[232] The CyberPeace Institute investigates cyberattacks, identifying the tactics, techniques and procedures involved and producing reports to assist investigators.[233]

---

228 See, for example, Europol (undated), 'Partners & Collaboration' (updated 28 July 2025), https://www.europol.europa.eu/partners-collaboration.
229 ITU (undated), 'National CIRT', https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx (accessed 20 Nov. 2025). The term 'CERT', which stands for 'Computer Emergency Response Team', is often used interchangeably with 'CIRT'.
230 The Points of Contact Directory was set up by the UN's Open-Ended Working Group (OEWG) on the security of and in the use of information and communication technologies to establish secure and direct communications on malicious cyber incidents. So far, over 100 countries have joined. See UNIDIR (undated), 'Welcome to the Global Intergovernmental Points of Contact Directory on the Use of Information and Communications Technologies in the Context of International Security', https://poc-ict.unoda.org.
231 MITRE Corporation (undated), 'MITRE ATT&CK ', https://attack.mitre.org.
232 See, for example, National Cyber Security Centre (2024), 'SVR cyber actors adopt tactics for initial cloud access', advisory note, 26 February 2024, https://www.ncsc.gov.uk/news/svr-cyber-actors-adapt-tactics-for-initial-cloud-access.
233 CyberPeace Institute (undated), 'Data-driven accountability', https://cyberpeaceinstitute.org/threat-analysis/#threat-analysis-investigate.

A multi-agency approach is helping to disrupt cybercrime and assist investigations in that context. For example, Europol's 'Operation ENDGAME', involving several states, technology companies and Eurojust, is the largest ever operation against botnets used to facilitate major ransomware attacks. In 2024 and 2025, it led to multiple arrests, as well as the take-down of hundreds of servers.[234]

However, while cyber-enabled international crimes and cybercrime have issues in common, the prosecution of cyber-enabled international crimes brings extra challenges. Evidence may be harder to obtain from other states compared to a case involving a criminal gang operating a cross-border phishing scam, which states have a mutual interest in prosecuting. There will also be additional elements to prove in relation to international crimes, as noted elsewhere in this paper.

Since many states lack the resources to prosecute international crimes on their own, international organizations have an important role to play. As well as cybercrime teams, Europol, Interpol and Eurojust each have teams dedicated to facilitating cooperation between states (and between states and other actors) on the investigation and prosecution of core international crimes. The European Network for investigation and prosecution of genocide, crimes against humanity and war crimes (Genocide Prosecution Network) facilitates cooperation between national authorities on international crimes through national contact points, comprising specialized and dedicated prosecutors, investigators and officers for mutual legal assistance.[235] Europol, Eurojust, the EU's SIENA system and Interpol's I-24/7 system all offer platforms for cross-border cooperation, enabling real-time exchange of data between jurisdictions.

The benefit of joint investigations

The criminal investigation by the Joint Investigation Team (JIT) into the 2014 downing of Malaysian Airlines flight MH17 in Ukraine shows that joint investigations can be effective in cases involving complex attribution issues and technical evidence. The MH17 JIT investigation consisted of police and judicial authorities from Australia, Belgium, Malaysia and the Netherlands, working with Ukrainian authorities. It led to the identification of perpetrators and those responsible in the chain of command and resulted in the prosecution of four suspects. Three of those suspects were eventually found guilty and sentenced to life imprisonment.[236]

Eurojust helps to set up JITs and provides operational, legal and financial support to them.[237] The JITs Network encourages and promotes best practice in the use of JITs.[238] JITs are likely to be particularly helpful in relation to complex factual and legal situations, such as a state-sponsored cyber operation against critical

---

234 Europol (2025), 'Operation ENDGAME strikes again: the ransomware kill chain broken at its source', press release, 23 May 2025, https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source.
235 Eurojust (undated), 'Genocide Prosecution Network', https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/genocide-network.
236 Netherlands Public Prosecution Service (undated), 'The criminal investigation by the joint investigation team', https://www.prosecutionservice.nl/topics/mh17-plane-crash/criminal-investigation-jit-mh17.
237 Eurojust (undated), 'Joint investigation teams', https://www.eurojust.europa.eu/judicial-cooperation/instruments/joint-investigation-teams.
238 Eurojust (undated), 'JITs Network', https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/jits-network.

infrastructure that reaches the level of an international crime. There is scope for private companies to participate in joint investigations as technical experts, provided there are measures in place to prevent potential conflicts of interest.

Joint investigations can also help to lessen political sensitivities in relation to the prosecution of international crimes, as by acting collectively states may be more resilient to domestic pressures or retaliation from the accused state than if acting in isolation. However, joint investigations also require states to pool and cede some sovereignty and independence, so trade-offs are required. States must also have the authority to participate under their domestic law, which may be an impediment for some without legislative amendments.

Within a month of Russia's invasion of Ukraine in February 2022, a JIT was established to investigate core international crimes committed by Russia in Ukraine. The Ukraine JIT involves the national prosecution authorities of seven countries – Estonia, Latvia, Lithuania, Poland, Romania, Slovakia and Ukraine – and receives support from Eurojust, Europol,[239] the ICC, the Core International Crimes Evidence Database and the International Centre for the Prosecution of the Crime of Aggression against Ukraine (ICPA).[240] Being part of the Ukraine JIT has enhanced the OTP's ability to access and collect information in relation to the situation in Ukraine, as well as to conduct rapid coordination with partner countries.[241]

In its assault on Ukraine, Russia is using cyber technology in combination with physical military activity, some of which is alleged to amount to international crimes.[242] The UK government's statement on the recent sanctioning of three Russian GRU units and 18 military intelligence officers asserts that 'online reconnaissance' was used to guide Russian missile strikes on the Mariupol Theatre in which hundreds of civilians, including children, were killed.[243]

As armies become more reliant on the use of technology, we can expect to see international crimes increasingly committed using cyber and physical activity in concert. It is therefore crucial that investigations and prosecutions adapt to this modern reality.

---

239 In November 2023, Europol set up an OSINT taskforce to support investigations into war crimes committed in Ukraine. This taskforce, which has 14 participating countries, including the US, the UK and some EU member states, aims to identify suspects and their involvement in core international crimes in Ukraine through the collection and analysis of open-source intelligence. The taskforce supports requests from Ukraine, other countries and the ICC. See Europol (2023), 'Europol sets up OSINT taskforce to support investigations into war crimes committed in Ukraine', press release, 21 November 2023, https://www.europol.europa.eu/media-press/newsroom/news/europol-sets-osint-taskforce-to-support-investigations-war-crimes-committed-in-ukraine.
240 Eurojust (undated), 'Joint investigation team into alleged crimes committed in Ukraine', https://www.eurojust.europa.eu/joint-investigation-team-alleged-crimes-committed-ukraine. The US has been engaged through a memorandum of understanding, but withdrew from ICPA in March 2025.
241 See ICC Policy on Complementarity and Cooperation, p. 41ff; ICC (2024), '*Situation in Ukraine*: ICC-01/22', https://www.icc-cpi.int/situations/ukraine.
242 Human Rights Watch, SITU and Truth Hounds (2024), '"Our City was Gone": Russia's devastation of Mariupol, Ukraine', 8 February 2024, https://www.hrw.org/feature/russia-ukraine-war-mariupol/report.
243 Foreign, Commonwealth & Development Office and The Rt Hon. David Lammy MP (2025), 'UK sanctions Russian spies at the heart of Putin's malicious regime', press release, 18 July 2025, https://www.gov.uk/government/news/uk-sanctions-russian-spies-at-the-heart-of-putins-malicious-regime.

05 Conclusion and recommendations

All parties must ensure that they understand the applicability of international law to cyber-enabled international crimes, and should take steps to strengthen accountability for those crimes.

Although the law could further be clarified, it is clear that existing international criminal law applies to cyber-enabled international crimes. The OTP's policy paper will ensure that cyber-enabled international crimes are given due attention by the ICC. As this Chatham House paper has shown, states can also assert jurisdiction over these crimes.

Governments, prosecuting authorities, technology companies and civil society groups, among others, need to be fully aware of the ways in which the law applies to ICTs of all kinds. They also need to be aware of potential responsibility under international criminal law, including where the perpetrator is not the principal criminal but is assisting or facilitating in some way.

Cooperation between different entities (states, international organizations, private companies and civil society) will be crucial to the effective investigation and prosecution of cyber-enabled international crimes. Harmful cyber incidents have impacted all regions, causing disruption of essential services, economic loss and psychological trauma. This shared experience could provide the basis for a more global and proactive approach to bringing perpetrators to justice.

While recognizing the difficulties in investigating and prosecuting *any* cyber-enabled crime, the following section presents a series of recommendations to a range of stakeholders for strengthening accountability for cyber-enabled international crimes within both national and international law frameworks.

Recommendations

For states

States should use their best efforts to prevent the commission of cyber-enabled international crimes, including by non-state actors operating from their territory. As well as having binding obligations to do so in certain circumstances,[244] the UN voluntary norms on responsible state behaviour in cyberspace – agreed by the UN GGE in 2015 and since affirmed by the UN OEWG and many international bodies – set out the expectation that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.[245]

States should set out how they consider international criminal law applies in the cyber context by publishing or updating national position statements. If international criminal law is to constrain, deter and provide accountability for the gravest forms of cyber harm, there needs to be clarity on how the rules apply.

States should incorporate international crimes into their domestic law and provide appropriately wide jurisdictional grounds for prosecution, including when crimes are committed by cyber means. **They should also ensure that their domestic law enables them to participate fully in the joint investigation of international crimes.**

States should embed cyber expertise across national prosecution authorities. For example, they could appoint a cyber liaison expert, whose role would be to ensure lessons and expertise are shared between cybercrime and international crime teams; to explore avenues for informal information-sharing; and to promote effective liaison with international organizations on issues related to cyber-enabled international crimes.

State investigators and prosecutors should strengthen their informal networks with the cyberthreat intelligence community and CIRTs to increase their access to cyber intelligence. One way of strengthening such networks is through participation in reputable cyber networks and conferences such as Europol's annual Cybercrime Conference or the Council of Europe's 'Octopus' Conference on Cybercrime.

States should cooperate fully with the ICC and with intergovernmental organizations (such as Eurojust and Europol). As and when states amend their domestic law to implement new treaties relevant to the investigation and prosecution of cybercrime, such as the Second Additional Protocol to the Budapest Convention or the UN Convention against Cybercrime, **they should include the ICC in their cooperation mechanisms – for example, as one of the parties able to participate in JITs, or able to request material from states and other actors.**

---

244 For example, article 1 of the Convention on the Prevention and Punishment of the Crime of Genocide.
245 Digwatch (undated), 'UN Cyber Norm C: Prevent misuse of ICTs in your territory', https://dig.watch/cyber-norms/prevent-misuse-of-icts-in-your-territory. Some states and commentators consider that states are under a binding obligation to carry out due diligence in this respect. See Cyber Law Toolkit (undated), 'Due Diligence', https://cyberlaw.ccdcoe.org/wiki/Due_diligence.

Law enforcement officials can strengthen the prospect of successfully obtaining evidence from technology companies for the prosecution of cyber-enabled international crimes by **taking into account international human rights law and potential conflicts of law when framing their requests for evidence, and ensuring they have rule-of-law safeguards in place for handling the evidence they receive.**[246]

States should put in place the necessary internal procedures and international arrangements to strengthen cooperation in the investigation and prosecution of both cybercrimes and cyber-enabled international crimes. To do so, they may wish to consider becoming parties to existing treaties, such as the Second Additional Protocol to the Budapest Convention and the UN Convention against Cybercrime, or to conclude new bilateral treaties with partner states.

In implementing their obligations under cybercrime treaties, **states parties should ensure that they comply with their obligations under international human rights law**, including procedural safeguards.

For the OTP

If budget permits, **the OTP should reinforce its existing in-house cyber expertise**, with the aim of deepening its technical knowledge of the threat and forensics landscape (including digital forensics, attribution, encryption and blockchain-tracing), as well as enhancing its knowledge of the legal and regulatory landscape, including the navigation of cross-border frameworks for data sharing.[247] This would fit with the court's proposed thematic approach to cyber issues and its acknowledgment that the pervasive nature of information technology means that, increasingly, many if not all criminal investigations will likely have a cyber component.[248] In light of this approach, **the recruitment of additional, dedicated staff should form the basis of a powerful funding request to states.**

If funds are not available, a suggestion in the OTP's policy paper of expanding secondments from outside the ICC is a good alternative.[249] **These should be long-term secondments of lawyers and/or other relevant experts**, particularly those who understand the regulatory schemes around gathering digital evidence. In establishing such secondments, measures to avoid possible conflicts of interest should be put into place.

In its policy paper, the OTP anticipates outsourcing at least some of the forensic analysis necessary in complex cases,[250] and commissioning specific advice from third party providers where appropriate.[251] For the investigation of complex cyber operations, the OTP could **commission reports from a cybersecurity provider**

---

246 The Trusted Cloud Principles initiative set out the principles under which signatory companies (including Amazon, Google and Microsoft) seek to provide information transparently, and in accordance with the rule of law and human rights standards. See Trusted Cloud Principles (2021), 'Principles', https://trustedcloudprinciples.com/principles.
247 The OTP policy paper notes the OTP's intention to 'continue to recruit staff with required breadth and depth of experience relevant to the work of the Office, including facility with technical and digital evidence'. See ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 143.
248 Ibid., para 23.
249 Ibid., paras 114 and 159.
250 Ibid., para 159.
251 Ibid., para 140.

in relation to actors of interest to the court – for example, those operating in an area already under investigation. This type of collaboration would provide a structured basis for cooperation with cybersecurity firms, which can offer capabilities that the OTP cannot sustain in-house (such as malware analysis, attribution and dark web monitoring) and give prosecutors valuable leads. In its dealings with these and other external actors, the OTP should be vigilant in upholding its independence at all times.

While the OTP already has cooperation arrangements in place with Eurojust and Europol, **there is scope for enhanced cooperation between the OTP and the EU.** A formalized agreement or liaison mechanism could help to strengthen further the OTP's access to the EU's technology expertise, evidence and networks. **The OTP should also explore joining the EU's SIRIUS network** to facilitate access to cross-border electronic evidence, as well as knowledge-sharing and best practice.

The OTP should identify opportunities for outreach and cooperation on the prosecution of cyber-enabled international crimes beyond the EU. As well as helping to sensitize these regions to the OTP policy position, broader cooperation would minimize the risk of instrumentalization by any one regional group.

The OTP policy paper makes clear that the OTP will explore ways to enhance direct cooperation with all stakeholders, including private entities.[252] This will include the creation of a standing mechanism to ensure that the OTP can benefit from dialogue with experts in this area, 'including but not necessarily limited to civil society and industry experts'.[253] **As part of this mechanism, it would be valuable for the OTP to include specialists in digital forensics, digital infrastructure and cyberthreat intelligence**, as well as representatives from Europol and Interpol.

The OTP should also explore the possibility of joining public–private partnerships already formed by certain states and regional organizations – for example, the partnerships forged by Europol, Interpol and ENISA with trusted technology and cybersecurity companies.

The OTP should consider establishing a forum for technology exchanges and capacity building as a platform for information exchange between the OTP and private actors. Such a forum could help to demystify the investigation and prosecution process, and build greater trust and understanding between the OTP and private actors. It would not only be useful for the major US technology companies, but also for smaller technology companies that are not as well-resourced or familiar with issues in this area, as they respond to requests for evidence.

For private companies

Companies should carry out human rights due diligence, the need for which is heightened when companies are operating in conflict-affected contexts.[254] All companies – including social media platforms, cloud providers, satellite companies,

252 Ibid., para 193.
253 Ibid., para 140.
254 UNDP (2022), *Heightened Human Rights for Business in Conflict-Affected Contexts: A Guide*, guidebook, https://www.undp.org/publications/heightened-human-rights-due-diligence-business-conflict-affected-contexts-guide.

providers of surveillance technology and cryptocurrency exchanges – should uphold the corporate responsibility to respect human rights, including by not causing or contributing to adverse impacts on any human rights through their activities.[255]

Companies' due diligence processes should include procedures to identify and mitigate the risks of participation in harmful cyber activity that violates international law, including international criminal law. ICT companies should have policies in place for staff to report concerns about potential complicity in international crimes. Training policies should include the circumstances in which company directors and other members of staff may be liable under international criminal law, in addition to domestic cybercrime law. **Companies should also participate in external training provided by reputable bodies in this area** (for example, the OTP or Eurojust).

Where there is a serious risk of international crimes being committed, **technology companies should preserve any material taken down on their own initiative to ensure it is available for investigators at a future date**. Technology companies have a responsibility to cooperate with investigators and prosecutors on the preservation and production of evidence relevant to cyber-enabled international crimes. But in certain circumstances, technology companies may decide to take down material in line with their own terms of service or in response to legal concerns. In such cases, retention should be the default.

Technology companies should ensure they have law enforcement portals in place to facilitate timely responses to requests for evidence of international crimes.

Companies should also work together to standardize the systems they use to process such requests to make those processes more efficient.

For civil society organizations

Civil society organizations, including NGOs, universities and think-tanks, should facilitate multi-stakeholder dialogue on the practical issues involved in preserving and sharing evidence of cyber-enabled international crimes. As the Chatham House roundtables found, this will not only help to build relationships between different stakeholders, but also to develop shared understandings of the constraints and possibilities in this area.

When collecting evidence relevant to the prosecution of international crimes, **civil society organizations should aim to follow protocols designed by the ICC and others that provide standards on the collection and use of digital evidence in court**, to increase the likelihood that such evidence is admissible in court.

Civil society organizations or academics should establish a database with details of all domestic or international investigations and prosecutions of cyber-enabled international crimes, both past and ongoing. Such a database would ensure that relevant information is easily available in one place, providing a repository of know-how for all relevant actors.

---

255 OHCHR (2012), *The Corporate Responsibility To Respect Human Rights: An Interpretative Guide*, https://www.ohchr.org/sites/default/files/Documents/Publications/HR.PUB.12.2_En.pdf.

For all parties

States and civil society should support the OTP in its efforts to brief and train external partners in this area, including those in the private sector. As the OTP policy paper notes, there is a need for outreach by the OTP to familiarize all actors with cyber-enabled criminality under the Rome Statute and facilitate future cooperation.[256]

States and the OTP should ensure that adequate training is available to investigators, prosecutors and judges in digital forensics, attribution, encryption, blockchain-tracing and deepfake detection, as well as legal and regulatory expertise in cross-border frameworks, data localization laws and admissibility standards for evidence. This would benefit the prosecution of all crimes with a digital element.

Training in the prosecution of cybercrime provided by organizations such as Eurojust, the Genocide Prosecution Network, the European Judicial Training Network and the Cybercrime Programme Office of the Council of Europe should be adapted to include the prosecution of cyber-enabled international crimes, and the OTP should be invited to take part. Table-top exercises that work through case studies are particularly valuable in relation to complex cyber cases.

States, international organizations and NGOs should work together to establish regional networks, along the lines of the recently established PacificJust,[257] that can facilitate the operation of JITs in other parts of the world. To date, efforts to coordinate joint investigations into international crimes have been dominated by European institutions. To enable a wider range of states from different regions to participate in joint investigations, there will need to be investment in capacity and institutions beyond Europe.

States should invest in advanced eDiscovery systems (akin to those already in use by civil litigators) to enable their prosecuting authorities to properly store, authenticate and analyse digital evidence. Many national prosecution services currently lack the facilities necessary to handle significant amounts of digital data. Investment in such systems can be useful for the investigation of a range of other crimes, as well as for cyber-enabled international crimes. Meanwhile, the ICC and states that already have digital evidence management systems should keep those systems under review to ensure they remain resilient, robust and relevant.

256 ICC Office of the Prosecutor (2025), *Policy on Cyber-Enabled Crimes under the Rome Statute*, para 145.
257 The Pacific Justice Network for the investigation and prosecution of core international crimes (PacificJust) was established in October 2024. See PacificJust (undated), 'Home', https://www.pacificjust.org.

About the authors

Elizabeth Wilmshurst CMG KC is a distinguished fellow in the International Law Programme at Chatham House. She first joined the institute in 2004 when she set up the programme, and then became an associate fellow, as well as being a part-time professor of international law at University College London. She had previously served as a legal adviser in the UK diplomatic service between 1974 and 2003. Between 1994 and 1997, she was the legal adviser to the UK mission to the UN in New York.

Elizabeth took part in the negotiations for the establishment of the International Criminal Court. Her experience has been in public international law generally, with a particular emphasis on the use of force, international criminal law, the law of the UN and its organs, and international humanitarian law.

Harriet Moynihan is head of accountability in international law at the Oxford Institute of Technology and Justice in the Blavatnik School of Government, University of Oxford. Harriet's work focuses on accountability for malicious cyber operations and on the use of technology, including AI tools, to strengthen accountability processes.

Harriet is also an associate fellow in the International Law Programme at Chatham House (of which she was formerly the director) and a research affiliate at the Oxford AI Governance Initiative of the Oxford Martin School, University of Oxford. Harriet previously worked for eight years as a legal adviser in the UK's Foreign & Commonwealth Office, and prior to that practised as a competition lawyer at Clifford Chance LLP.

Dr Tsvetelina van Benthem is a lecturer in international law at the University of Oxford and a lecturer in law at the University of Reading. Her research focuses on the application of international law to emerging technologies, including AI and ICTs. She is a core team member of the Oxford Process on International Law Protections in Cyberspace, a member of the Sino-European Expert Working Group on the Application of International Law in Cyberspace, and a 'red-team' reviewer of the West Point Manual on the International Law Applicable to Artificial Intelligence in Warfare.

Tsvetelina is also a senior legal adviser at The Reckoning Project. In this capacity, she routinely engages with domestic and international accountability mechanisms on matters concerning violations of international humanitarian law, international criminal law and human rights law.

Acknowledgments

The authors would like to thank the participants in the roundtable meetings, held under the Chatham House Rule, who gave generously of their time and provided valuable insights. Particular thanks are due to Marko Milanovic, Miles Jackson, Lindsay Freeman and the anonymous peer reviewer for their comments on this paper. The views expressed in the paper are the sole responsibility of the authors. Chatham House is grateful to the various funders who gave support for this project.

Cover image: A person walks behind a glass wall displaying machine-coding symbols in Moscow, 17 October 2016.
Photo credit: Copyright © Kirill Kudryavtsev/AFP/Getty Images

ISBN 978 1 78413 663 5
DOI 10.55317/9781784136635

Cite this paper: Wilmshurst, E., Moynihan, H. and van Benthem, T. (2026), *Securing justice for cyber-enabled international crimes: Legal foundations and practical routes to prosecution*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784136635.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223