Introduction to the

Oxford Process on International Law Protections in Cyberspace

The Oxford Process on International Law Protections in Cyberspace, convened by Professors Dapo Akande and Duncan Hollis, is an initiative of the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) at the Blavatnik School of Government. It was set in motion in May 2020 in partnership with Microsoft and the Government of Japan.

The Oxford Process is a collaborative effort of leading international legal experts from across the Globe to build consensus around international law protections in cyberspace. Aimed at identifying and clarifying the rules of international law applicable to cyber operations targeting particular objects of protection or using particular methods, it seeks to move beyond the assertion that international law applies in cyberspace and to clarify the extent to which and how it does so. The Process responds to the most urgent problems facing the international community with respect to information and communications technologies and their cyber environment.


Background

Cyber threats are on the rise as we witness the normalization of cyber insecurity. Since the start of 2020, cyber operations have targeted, among many others, electric power utility companies and telecommunication services in Latin America, hospitals and vaccine research facilities across Europe and Asia, governmental structures and the financial sector in many African countries, essential services, such as water and energy supply, in North America and the Asia-Pacific region, as well as information and communications technology companies mostly based in the United States. These cyber threats know no frontiers, and they imperil the security of states, economic activity, and individuals worldwide.

Our increasing dependence on the Internet and other digital technologies means that hardly any sphere of life has remained untouched by this constant stream of nefarious cyber activity. Attacks crippling the functioning of hospitals, research institutes and water filtration plants endanger lives and livelihoods. Privacy is becoming more of an aspiration than a reality, with personal data compromised following IT supply chain attacks, or exposed through hacks on dating apps later shared on the Darknet. Information campaigns tamper with electoral processes, manipulating and intimidating voters. A raging infodemic has accompanied the pandemic. Amplified by inter-connectivity and digital tools, manipulated information travels fast and reaches far. Ransomware, insidious and inherently coercive, drains and disrupts businesses and institutions. Looking at the operations from the past two years, little, if anything, seems to be off limits.

What consequences flow from this rise and proliferation of harmful cyber operations?

First, trust, a key component of any functioning society, including the international one, is now under attack. Cyber activities undermine trust in institutions, humanitarian organisations, IT supply chains, electoral processes and scientific communities.
Second, although a matter of mere speculation in the past, direct effects, such as damage, disruption, distress are now becoming clearly observable.

Third, the rise and proliferation of harmful cyber operations have also led to their increased sophistication. Packaged malware is becoming harder to detect on targeted systems, while malicious exploits evade cyber defence vulnerabilities in novel ways.

Fourth, to counter these trends, more public and private resources have necessarily been directed towards the patching of vulnerabilities, building of robust cybersecurity, and educational campaigns on cyber hygiene. Ensuring a secure cyberspace comes at a high financial cost and may require diversions of funds from other areas that are important to public life. Such trade-offs notwithstanding, there is a growing awareness and acceptance that cyber security is a precondition for the normal functioning of societies.

A fifth and final consequence is that, in a space that is becoming increasingly uncertain due to evolving risks of harm, the need for legal certainty is pressing and acute. When is certain activity permitted and when it is plainly illegal? When and to what extent must cyber operations be prevented or remedied? Both states and other stakeholders have coalesced around the view that international law – a growing regulatory framework governing international and domestic affairs – has a crucial role to play in ensuring this legal certainty. Greater clarity on the protective reach of international law, via its prohibitions, permissions, and requirements, can exercise a pull towards compliance by all actors within this system. That compliance can, in turn, facilitate reduction in harmful cyber activities, as well as prevention, mitigation and redress for harms caused. As the March 2021 Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security (OEWG) concluded, ‘additional neutral and objective efforts to build capacity in the area of international law’ are needed to deepen understanding of how international law applies to the use of information and communication technologies.

In sum, the dramatic rise of cyberthreats has increased the demand for clearly stated rules of international law. Over the past two years, the Oxford Process on International Law Protections in Cyberspace has sought to respond to this growing need. It represents an effort to deepen understanding on the application of international law and to provide clarity on how this body of law governs and prohibits specific types of cyber operations. As an academic effort with government and industry support, the Oxford Process also reflects the importance of state engagement with multiple stakeholders, emphasized in the May 2021 consensus report of the Group of Governmental Experts on Advancing Responsible State behaviour in cyberspace in the context of international security (GGE). Such multi-stakeholder efforts at defining norms of international law in this area, the GGE cautioned, are ‘critical to bridging existing divides within and between States on policy, legal and technical issues relevant to ICT security.’

### The Oxford Process at a glance

The Oxford Process on International Law Protections in Cyberspace, convened by Professors Dapo Akande and Duncan Hollis, is an initiative of the Oxford Institute for Ethics, Law and Armed Conflict (ELAC) at the Blavatnik School of Government that was set in motion in May 2020 in partnership with Microsoft and the Government of Japan. In the ensuing months, the Process has emerged as a collaborative effort among dozens of international legal experts from across the Globe, aimed at identifying and clarifying the rules of international law applicable to cyber operations targeting particular objects of protection or using particular methods.

Driven by urgent global problems, the goal of the Oxford Process is to move beyond the simple assertion that international law applies in cyberspace to clarify exactly how it does so. The Oxford
Process provides a platform for multi-stakeholder discussions and thereby, to articulate points of broad consensus on international legal rules. Over the course of 2020 and 2021, the Process has produced a number of major outputs, including five Oxford Statements on International Law Protections in Cyberspace, each of which articulates short lists of consensus protections that apply under existing international law. More than a hundred international lawyers from all continents have endorsed each of these statements. They have subsequently earned recognition by both public and private fora grappling with related problems.

| History |

In May of 2020, ELAC hosted a two-day virtual workshop, co-sponsored by Microsoft and the Government of Japan, entitled ‘Applying International Law in Cyberspace: Protections and Prevention’. This workshop occurred at a time of intensifying cyber operations against the healthcare sector, during a particularly worrisome and pernicious time of global pandemic. During the very rich workshop discussions, the participants examined a wide range of relevant international legal rules, both negative (that is, obligations to refrain from doing something) and positive (that is, obligations to do something or take certain steps to achieve certain results). Even in a virtual room filled with international lawyers – each with their own take on the existence and content of particular rules – agreement emerged in substance on a striking range of issues: international law prohibits cyber operations by states that have serious adverse consequences for essential medical services in other states. Divergence arose regarding how the participants reached this conclusion, with different experts placing reliance on a plethora of principles and rules, such as non-intervention, sovereignty, international humanitarian law, and human rights. But despite differences on the precise route taken, there was widespread agreement on the nature of the prohibited acts and the coverage of international legal protection, i.e. the substance of prohibited or required state behaviour.

It was this realisation – of agreement on protective coverage – that led to the first Oxford Statement that elaborated points of consensus on the protection of the healthcare sector. The ensuing four statements — the Oxford Statement on Safeguarding Vaccine Research, the Oxford Statement on Foreign Electoral Interference through Digital Means, the Oxford Statement on the Regulation of Information Operations and Activities and the Oxford Statement on the Regulation of Ransomware Operations. These Statements reflect the uniqueness of the Oxford Process with its singular focus on clarifying the rules of international law applicable to cyber operations targeting particular objects of protection or using particular methods. Beyond the five workshops that led to Statements, the Process also convened two additional events to dive deeper into the due diligence component of the Oxford Process (which is incorporated in each of the Five Statements) through a workshop on ‘Cyber Due Diligence Obligations in International Law: Theory and Practice’ and a workshop focused on another object of protection: IT Supply Chains. Each of these events generated an Oxford Process Report, detailing the workshop presentations, discussions, and areas of agreement.

| Methodology |

The methodological approach of the Oxford Process is its distinctive feature, and one which clearly distinguishes it from other academia-led initiatives in the field of international legal regulation of cyber operations. This approach has three main characteristics: it is 1) based on consensus; 2) inquiring into the application of international law to specific objects and methods; 3) responding to urgent problems facing the international community.

1) Articulating points of consensus
The Oxford Process articulates points of consensus (the ‘low-hanging fruit’) without necessarily being prescriptive about the particular principles or rules of international law that underlie conclusions on the scope of legal protection. In this way, the emphasis is on unity, not on differences.

2) International law applied to specific objects and methods

Rules of international law are not discussed in the abstract. The Oxford Process looks at specific objects and areas of protection, as well as particular methods of conducting cyber operations. This is important, as the means and ends of cyber protections inform and concretise the ways in which international law regulates particular operations. For that reason, the first Oxford Statement focused on healthcare, the second on vaccine research, the third on electoral processes, the fourth on information operations and activities, and the fifth on ransomware. The first three Statements centred around specific objects or areas of protection, while the last two transitioned to identifying particular forbidden methods of cyber operations.

3) Responding to urgent global problems

Being guided by discrete needs triggered by specific events has grounded the Process in the current reality of cyber operations and cyber-related harms. Hence, technical and policy experts are often invited to present at the workshops and encouraged to actively participate in the discussions. This wealth and diversity of real-life and real-time expertise facilitates the connection between international legal rules and the reality of cyber operations, thus allowing a deeper understanding into the types of concrete harms that such operations can cause and the measures that can and are being taken to prevent, mitigate and redress harms.

For example, at the very start of the July 2020 workshop aimed at clarifying the protection of vaccine research, a technical cybersecurity expert introduced the participants to the types of harm that accompany even the mere entry into networks that contain trial data on vaccines (including the possibility of needing to fail that trial), disrupting the conventional wisdom of international lawyers that losses of confidentiality alone can never cause a loss of integrity to the targeted system. This led to a Statement that identified the act of penetration into vaccine research systems or databases as a *per se* harm. Similarly, during the IT Supply Chains workshop, the group, guided by an expert from the private sector, dived into the mechanics of the SolarWinds hack, including the way in which the malware became part of the build and received the digital certificate of the provider. All of these details assisted in shaping the discussions, as they clarified the precise form that malicious cyber operations now take and the precise types of harm to which they can give rise.

From a procedural standpoint, each Oxford Statement is drafted and revised following rich and rigorous workshop discussions, as well as subsequent, additional feedback received from workshop participants. Once a Statement is finalised, it is opened for signature, first to the workshop participants and previous Signatories. Then, the Statement is publicised through various academic and media platforms, including the blog of the European Journal of International Law (EJIL Talk!), Opinio Jusris and Just Security. These publications not only disseminate the content of each Statement but also invite other international lawyers to sign them. In short, all Statements followed the same five-stage process: convening of workshop → discussions → emerging consensus → consensus embodied in a brief Statement → publication.

<table>
<thead>
<tr>
<th>Substantive features of the Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>A strong substantive focus underlies and defines the Oxford Process. Beyond articulating applicable areas of international law and specific rules, it seeks to provide states and other stakeholders with concrete guidance on what behaviour is expected from them. Three substantive...</td>
</tr>
</tbody>
</table>
features flow from this goal. First, the Process clarifies not only negative, but also positive obligations under international law, placing the latter front and centre in ensuring the protection of essential objects, services and processes. Second, it seeks to identify the rules applicable not only to states, but also to other actors bound directly by international law. Third and finally, it is comprehensive in that it examines obligations applicable in both peacetime and times of conflict.

**Clarifying positive obligations**

The Oxford Process focuses not only on prohibitive rules of international law, but also on rules that require states to take particular positive steps to prevent, mitigate and redress illegal interference. Both types of rules receive equal attention and are given equal importance. All five Oxford Statements shed light on the general scope of positive obligations under international law, while at the same time detailing concrete measures that states could adopt to fulfil these obligations. For instance, the Oxford Statement on the Regulation of Ransomware Operations concluded that

> ‘States must take measures to protect the human rights of individuals within their jurisdiction from harmful ransomware operations, including when such operations are carried out by other states and non-state actors. To discharge this obligation, states may, among other measures, prohibit ransomware by law, take feasible steps to stop ransomware operations, mitigate their effects, investigate and punish those responsible, as well as prevent and suppress ransom payments to the extent possible. Where such protective measures interfere with other human rights, they must conform with applicable legal requirements, such as legitimate purpose, legality, necessity, proportionality and non-discrimination.’

The Process takes a results-based approach, whilst highlighting that positive measures must not themselves be used as justifications for breaches of international law. Thorough and rigorous research on obligations containing a due diligence standard has accompanied the Oxford Process from its inception, with insights finding their way both into the Oxford Statements and separate workshops and publications.

**Looking beyond states**

States are not the only actors bound directly under international law. Mindful of this, and of the importance of clarifying the obligations of all relevant actors, the Oxford Statements have consistently outlined obligations that bind individuals and parties to conflict (not only states parties, but also non-state actors). For instance, the Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector concluded that

> ‘During armed conflict, international humanitarian law requires that medical units, transport and personnel must be respected and protected at all times. Accordingly, parties to armed conflicts: must not disrupt the functioning of health-care facilities through cyber operations; must take all feasible precautions to avoid incidental harm caused by cyber operations, and; must take all feasible measures to facilitate the functioning of health-care facilities and to prevent their being harmed, including by cyber operations.

> 6. Cyber operations against medical facilities will amount to international crimes, if they fulfil the specific elements of these crimes, including war crimes and crimes against humanity.’

**Protections in times of peace and armed conflict**

The Oxford Process seeks to provide a comprehensive picture of protections under international law. This means that the legal inquiries into the way in which international law applies to particular objects and methods extend across peacetime to times of armed conflict. Each of
these inquiries is tailored to the specific context of application. In the Oxford Statement on the Regulation of Information Operations and Activities, it was concluded that

‘The conduct of information operations or activities in armed conflict is subject to the applicable rules of international humanitarian law (IHL). These rules include, but are not limited to, the duty to respect and ensure respect for international humanitarian law, which entails a prohibition against encouraging violations of IHL; the duties to respect and to protect specific actors or objects, including medical personnel and facilities and humanitarian personnel and consignments; and other rules on the protection of persons who do not or no longer participate in hostilities, such as civilians and prisoners of war.’

**Outputs**

The outputs of the Oxford Process now take a variety of forms. The five Oxford Statements detailed in the previous sections spell out, in a clear and concise way, consensus protections under existing international law. In addition to the Statements, the Oxford Process produces Reports outlining the discussions that have taken place during the various workshops. In addition, a wide array of background papers and blog posts have been created for, or inspired by, the themes and conversations of the various Oxford Process workshops.

Though not written outputs *per se*, the workshops convened by the Oxford Process are a ‘product’ in and of themselves, as they provide a platform for dialogue across multi-stakeholder groups. Through these workshops, the Oxford Process has created its own ever-expanding community of experts. Furthermore, the workshops have served as a catalyst for further conversations on international legal protections, including areas in which differences of opinion persist and that thus require additional analysis. Each workshop has also spurred a search for the next topic for which the governing norms should be identified. For instance, the first workshop on the protection of the healthcare sector against malicious cyber operations prompted a more specific workshop on vaccine research and development subsequently. Similarly, the workshop on foreign electoral interference through digital means created momentum for a subsequent workshop on the broader issue of information operations and activities.

**The Oxford Process reflected in external events, processes and initiatives**

Although the Oxford Process was initiated less than two years ago, it has already carved out a space for itself front and centre on the radar of the international community. Support for the Oxford Process has come from legal experts around the world, including former judges of the International Court of Justice, United Nations (UN) Special Rapporteurs, and representatives of states. Each Oxford Statement has been signed by more than a hundred international lawyers, both public and private – a significant feat in an area where international legal regulation is so heavily contested. The accompanying infographics show that the success of the Oxford Process is the product of support coming from all regions.

Many UN events and processes over this past year and a half have featured discussions of the Oxford Process as an important and meaningful initiative in the area of cyber regulation. The first two Oxford Statements on the healthcare sector were cited during two UN Arria Formula Meetings on cybersecurity, with the Acting Assistant Secretary-General for the UN Office for the Coordination of Humanitarian Affairs mentioning these Statements in the context of important initiatives aimed at addressing how international law applies to cyber operations. The Process is also mentioned in key UN documents, such as the 2021 report of the UN Office on the
Coordination of Humanitarian Affairs, ‘From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action’.

Beyond these important acknowledgments, representatives of the Oxford Process are now regularly invited to present at various events in the sphere of cyber regulation including those associated with the Paris Call for Trust and Security in Cyberspace, as well as sessions with representatives of the Organisation of American States, the African Union, and the European Union, alongside state-organised workshops on particular areas of protection, such as Slovenia’s sponsorship of discussions on protecting water services and the financial sector, and Mexico’s Regional Consultation of Latin American States on International Humanitarian Law and Cyber Operations during Armed Conflicts, co-hosted with the International Committee of the Red Cross.

Simply put, the Oxford Process is now firmly established in the international legal sphere. As a norm-identifying and declaring process in a critical and fast-moving area, it complements other important initiatives, such as the UN GGE, OEWG and the Tallinn Manual processes, by adding its own unique approach to clarifying and spelling out existing protections.

<table>
<thead>
<tr>
<th>Who is behind the Oxford Process?</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Oxford Process is convened by Professor Dapo Akande (University of Oxford, Blavatnik School of Government) and Professor Duncan B. Hollis (Temple University). A small core team is working on both substantive issues and the planning and organisation of events. The team comprises Dr Antonio Coco (Essex), Dr Talita Dias (Oxford), Prof Harold Hongju Koh (Yale and Oxford), Mr James O’Brien and Mr Nikhil Sud (Albright Stonebridge Group), Dr Priya Urs and Ms Tsvetelina van Benthem (Oxford ELAC). Financial and organisational support has been provided by Microsoft and the Government of Japan. Beyond this core team, however, it is the thoughts, ideas, effort and time of hundreds of people that have made the Oxford Process what it is today. All Oxford Process workshops bring together a wealth of expertise from different sectors and disciplines. Initially, the workshops attracted primarily academics, but gradually, the composition of the events changed, with the latest ones being attended by representatives of more than ten states and several international and non-governmental organisations. The participating international legal experts hail from the widest range of geographic regions and legal systems; its experts come from all six inhabited continents – a testament to the importance of the topics reviewed, the global demand for this kind of norm-identification, and a basis for the diverse and representative discussions and outputs produced by the Process. Likewise, both Oxford Process’ core team and its other participants have brought together different generations of experts and practitioners, with a significant presence of female thought leaders in an area where they have been traditionally under-represented.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Looking ahead</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Oxford Process is a process in more ways than one. First and most obviously, it is a process of clarifying how international law applies to specific objects, areas and methods of cyber operations. Second, it is also a process of garnering consensus through its own distinctive methodology, through which an epistemic community is established and continuously expanded through repeated dialogue. Third, it is a process of combining expertise from different legal areas, while maintaining the rigorous disciplinary methodology for identifying, interpreting and applying international law. Fourth, it is a process committed to international law as a protector of objects, services and processes that are essential for the life, livelihood and dignity of individuals. With each workshop and Statement, the Process affirms that international law is not just an apology for</td>
</tr>
</tbody>
</table>
power. Rather, it expressly protects from harmful cyber operations the objects and sectors needed for the preservation and development of human life, health, privacy, expression, including the effective functioning of domestic institutions and essential services. Fifth and finally, it is a process of highlighting the benefits of collaboration, of debating, of navigating disagreements to discern points of consensus, of having all relevant stakeholders actively engaged and committed to a robust system of international legal protections.

Describing the fast-moving landscape of international legal rules in cyberspace is like describing what one sees from a moving train: the landscape changes as quickly, if not more quickly, than one can describe it. Such dynamic changes make the identification and application of international law challenging, but all the more necessary. In the future, the Oxford Process will continue to advance its mission of clarifying international legal rules in their application to the cyber context and responding to the most pressing problems of the day. One way of advancing this mission is to share, in an accessible way, all that has already been achieved through the Process in its first two years. This is the aim of the present publication. It contains all Oxford Statements, the posts accompanying their publication, the reports of all workshops and a list of all Oxford Statements Signatories. Committed to ongoing dialogues with states and other stakeholders, the Oxford Process team will continue to engage, support international processes, build capacity, expand its community of experts, seek consensus among diverging views, and respond to the evolving cyber landscape.
The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector

(Signatories: 139)

We, the undersigned public international lawyers, have watched with growing concern reports of cyber incidents targeting medical facilities around the world, many of which are directly involved in responding to the ongoing COVID-19 pandemic.

We are concerned that the impact of such incidents is exacerbated by the existing vulnerability of the health-care sector to cyber harm. Even in ordinary times, this sector is particularly vulnerable to cyber threats due to its growing digital dependency and attack surface.

We consider it essential that medical facilities around the world function without disruption as they struggle to respond to the COVID-19 pandemic. Any interference with the provision of health-care, including by cyber means, risks further loss of life as thousands continue to die every day.

We support the International Committee of the Red Cross’ call on States to protect medical services and medical facilities from harmful cyber operations of any kind.

We emphasize that cyber operations do not occur in a normative void or a law-free zone. As recognized by the United Nations General Assembly, international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology environment.

Guided by these considerations, we agree that the following rules and principles of international law protect medical facilities against harmful cyber operations. We encourage all States to consider these rules and principles when developing national positions as well as in the relevant multilateral processes and deliberations:

1. International law applies to cyber operations by States, including those that target the health-care sector.
2. International law prohibits cyber operations by States that have serious adverse consequences for essential medical services in other States.
3. International human rights law requires States to respect and to ensure the right to life and the right to health of all persons within their jurisdiction, including through taking measures to prevent third parties from interfering with these rights by cyber means.
4. When a State is or should be aware of a cyber operation that emanates from its territory or infrastructure under its jurisdiction or control, and which will produce adverse consequences for health-care facilities abroad, the State must take all feasible measures to prevent or stop the operation, and to mitigate any harms threatened or generated by the operation.
5. During armed conflict, international humanitarian law requires that medical units, transport and personnel must be respected and protected at all times. Accordingly, parties to armed conflicts: must not disrupt the functioning of health-care facilities through cyber operations; must take all feasible precautions to avoid incidental harm caused by cyber operations, and; must take all feasible measures to facilitate the functioning of health-care facilities and to prevent their being harmed, including by cyber operations.
6. Cyber operations against medical facilities will amount to international crimes, if they fulfil the specific elements of these crimes, including war crimes and crimes against humanity.
7. The application of the aforementioned rules of international law is without prejudice to any and all other applicable rules of international law that provide protections against harmful cyber operations.

(Signatories: 105)

As the COVID-19 crisis continues to affect millions of individuals around the world, the development of a vaccine becomes an essential component of States’ responses to the pandemic. A vaccine may not only save lives but also mitigate the socio-economic impact of the disease by allowing individuals to interact and work more safely.

Noting that, whilst the coronavirus pandemic and its consequences unfold, medical and research facilities in several countries have been targeted by malicious cyber operations, and that seemingly minor intrusions can disrupt or harm the availability or integrity of the data which could, among other things, compromise the ability to conclude clinical trials, obtain approval for them or manufacture or distribute an eventual vaccine,

Further noting that, because scientific development is now highly dependent on information and communications technologies spread across the globe, such harmful cyber activity may undermine States’ and global efforts to contain and recover from the COVID-19 pandemic and its side-effects,

Bearing in mind that COVID-19 is a highly contagious disease that respects no national borders, making international solidarity essential to restoring global health security,

Considering that the discovery and widespread provision of a safe and effective COVID-19 vaccine could save not just lives, but also economic livelihoods around the world,

Noting the Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector conclusion that ‘[a]ny interference with the provision of healthcare, including by cyber means, risks further loss of life as thousands continue to die every day’,

And emphasizing that — even if the specific application and interpretation of international law to the technologies, knowledge and data used in the process of vaccine development require fleshing out — COVID-19 vaccine, research, manufacture, and distribution are both essential medical services and part of States’ critical infrastructure that must be protected by international law,

Guided by these considerations, we agree that, currently, the following rules and principles of international law protect the research, manufacture and distribution of COVID-19 vaccine candidates against harmful cyber operations. We encourage all States to consider these rules and principles when developing national positions as well as in the relevant multilateral processes and deliberations:

1. As affirmed in the first Oxford Statement, international law applies in its entirety to cyber operations by States including those that target the healthcare sector and essential medical facilities. These facilities include vaccine research, trial, manufacture and distribution facilities, other research paths to therapies and preventative measures, together with their technologies, networks and data, particularly clinical trial results, and other research.

2. International law prohibits cyber operations by States that have significant adverse or harmful consequences for the research, trial, manufacture, and distribution of a COVID-19 vaccine, including by means that damage the content or impair the use of sensitive research data, particularly trial results, or which impose significant costs on targeted facilities in the form of repair, shutdown, or related preventive activities.
3. International humanitarian law requires that at all times parties to an armed conflict: (a) respect and protect medical facilities, transport and personnel, including those involved in COVID-19 vaccine research, trial, manufacture and distribution; (b) refrain from disrupting the functioning of COVID-19 vaccine research, trial, manufacture and distribution facilities in any way, including through cyber operations; and (c) take all feasible precautions to prevent and avoid, or at least minimize, incidental harm caused by cyber operations to those facilities, and (d) take all feasible measures to facilitate their functioning and prevent their being harmed, including by cyber operations.

4. Outside of armed conflict, international law imposes negative and positive obligations on States vis-à-vis other States and individuals that afford comprehensive protection to the research, trial, manufacture, and distribution of COVID-19 vaccine candidates.

5. States must take all feasible measures to prevent, stop and mitigate malicious cyber operations against the data or technologies used for COVID-19 vaccine research, trial, manufacture or distribution which they know or should have known emanate from their territory or jurisdiction.

6. States’ positive duties to ensure civil and political rights under international law require them to protect COVID-19 vaccine research, trial, manufacture and distribution to individuals subject to their jurisdiction.

7. The fulfilment of social, cultural and economic rights under international law requires States during a pandemic: (a) to ensure the manufacture and distribution of a COVID-19 vaccine in a lawful, fair, equitable, affordable and non-discriminatory manner; and (b) to cooperate to facilitate access to the vaccine by other countries.
The Oxford Statement on International Law Protections Against Foreign Electoral Interference through Digital Means

(Signatories: 173)

We, the undersigned public international lawyers, have watched with growing concern reports of cyber incidents targeting electoral processes around the world, including allegations of foreign state and state-sponsored interference. We also note that the COVID-19 pandemic raises additional challenges to ensuring the integrity of such processes.

Whereas:

Two prior Oxford Statements have described the rules and principles of international law governing cyber operations that threaten two areas of pressing global importance, namely the safeguarding of the health care sector and global vaccine research;

International law protects electoral processes, and efforts to interfere, including by digital means, with a state’s choice of its political leaders or other matters on which it has free choice contravene basic principles of the international order;

The Charter of the United Nations (UN) establishes sovereign equality and each state’s political independence as bedrock elements of the international system; the UN General Assembly has affirmed that no state “has the right to intervene directly or indirectly, for any reason whatever, in the internal or external affairs of any other state”; and the International Court of Justice has held that every sovereign State has the right “to conduct its affairs without outside interference”;

Article 25 of the International Covenant on Civil and Political Rights declares that “[e]very citizen shall have the right and the opportunity, without … unreasonable restrictions [t]o take part in the conduct of public affairs, directly or through freely chosen representatives; [t]o vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors”; electoral interference can infringe human rights protected under the International Covenant on Civil and Political Rights, the African Charter on Human and Peoples’ Rights, the American Convention on Human Rights, and the European Convention on Human Rights;

Other international instruments, such as the Paris Call for Trust and Security in Cyberspace (2018), have called on all stakeholders to “[s]trengthen their capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities”;

All efforts by states and others to prevent such malign interferences should be consistent with international law;

The International Law Commission’s 2001 Articles on State Responsibility establish that a state is responsible for the conduct of its organs or officials, as well as for conduct carried out by persons or groups acting on the instructions of, or under the direction or control of, the state;

In line with the UN Guiding Principles on Business and Human Rights, online intermediaries and digital media companies should “conduct due diligence to ensure that their products, policies and practices … do not interfere with human rights”, as recognised in the April 2020 Joint Declaration on Freedom of Expression and Elections in the Digital Age, adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, and OAS Special Rapporteur on Freedom of Expression.

As states and other stakeholders learn more about the ways in which foreign cyber actions can adversely affect domestic electoral processes and how best to address such harms, international
law can be further clarified and strengthened by state practice that becomes accepted as customary international law.

We affirm that all states are bound to act in accordance with the rules and principles identified below.

Applicability

1. International law applies to cyber operations by states, including those that have adverse consequences for the electoral processes of other states.
   a. “Electoral processes” refer but are not limited to processes for selecting or electing individuals for public office, referenda, and plebiscites. These include:
      i. Balloting: registering, casting, tabulating, or assuring the integrity of a ballot including voter registries, ballot security and integrity protocols, voting machines, and paper ballots;
      ii. Verifying: systems used for reporting, recording, verifying and auditing votes and results of an election;
      iii. Informing: public or private systems that provide an electorate with procedural information about how to participate in an electoral process, as well as substantive information, of whatever origin, related to an electoral process, including information on individuals or groups participating in electoral processes, such as candidates for elective office, political parties, or organizations.
   b. Adverse consequences, in the electoral context, include actions, processes or events that intervene in the conduct of an electoral process or undermine public confidence in the official results or the process itself. These actions include but are not limited to intrusions into digital systems or networks that cast doubt on the integrity of election data, such as votes and voter registers, as well as cyber operations against individuals and entities involved in the election.

Duty to Refrain

2. A state must refrain from conducting, authorising or endorsing cyber operations that have adverse consequences for electoral processes in other states. States must refrain from, inter alia,
   a. Interfering, by digital or other means, with electoral processes with respect to balloting or verifying the results of an election;
   b. Conducting cyber operations that adversely impact the electorate’s ability to participate in electoral processes, to obtain public, accurate and timely information thereon, or that undermine public confidence in the integrity of electoral processes.
   c. Conducting operations that violate the right to privacy, freedom of expression, thought, association, and participation in electoral processes.

Duty Not to Render Assistance

3. A state must not render assistance to cyber operations that it knows will likely have adverse consequences for electoral processes in other states.

Due Diligence

4. a. When a state is or should be aware of a cyber operation that emanates from its territory or infrastructure under its jurisdiction or control, and which may have adverse consequences for electoral processes abroad, that state must take all feasible measures to prevent, stop and mitigate any harms threatened or generated by the operation.
b. To discharge this obligation, states may, to the extent feasible, be required to, inter alia, investigate, prosecute or sanction those responsible, take measures to prevent or thwart operations spreading misleading or inaccurate information, and/or assist and cooperate with other states in preventing, ending, or mitigating the adverse consequences of foreign cyber operations affecting electoral processes.

c. The measures taken to discharge a state’s obligations should be carried out in full compliance with other rules of international law.

**Obligation to Protect Against Foreign Electoral Interference**

5. States have an obligation to protect and ensure the integrity of their own electoral processes against interference by other states. To discharge this obligation, states may be required to put in place electoral security measures, such as legislation and backup systems, as well as to secure the availability of public, timely and accurate information on electoral processes. Any restrictive measures taken by states that interfere with human rights must be in accordance with applicable legal requirements, such as legitimate purpose, legality, necessity, proportionality and non-discrimination.

6. These rules and principles are without prejudice to other applicable international rules and ongoing processes.
The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities

(Signatories: 121)

Reiterating the commitment expressed in the First, Second and Third Oxford Statements to clarify rules of international law applicable in the use of information and communication technologies;

Considering that information operations and activities conducted by States or non-State actors through information and communications technologies have the potential to cause harm to both States and individuals, in light of their ability to reach a very wide audience instantly as exemplified by false claims surrounding COVID-19 treatments, vaccines, masks and social distancing; false or distorted claims directed at manipulating electorates or altering perceptions of climate change and technological developments; and by the incitement of violence, especially during armed conflict and periods of instability;

Understanding that the expression ‘information operation[s] and activities’ encompasses any coordinated or individual deployment of digital resources for cognitive purposes to change or reinforce attitudes or behaviours of the targeted audience;

Such information operations and activities include the dissemination of disinformation, misinformation, hate speech, other types of harmful speech and methods for their dissemination;

Recognizing that, as noted by the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights Special Rapporteur on Freedom of Expression and Access to Information, in their 2017 Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda, "disinformation and propaganda are often designed and implemented so as to mislead a population, as well as to interfere with the public’s right to know and the right of individuals to seek and receive, as well as to impart, information and ideas of all kinds, regardless of frontiers, protected under international legal guarantees of the rights to freedom of expression and to hold opinions" and that "some forms of disinformation and propaganda may harm individual reputations and privacy, or incite to violence, discrimination or hostility against identifiable groups in society";

Emphasizing that, as referenced in Principles 11 and 12 of the UN Guiding Principles on Business and Human Rights, companies have a responsibility to respect the human rights of individuals, and affirming that this responsibility extends to the impact of information operations and activities conducted using their services;

We agree that:

1. International law applies to all conduct carried out through information and communications technologies, including information operations and activities.

2. States must refrain from conducting information operations and activities when they would violate the principles of sovereignty and non-intervention in a State’s internal or external affairs.

3. States must refrain from engaging in, supporting or allowing forms of speech within their jurisdiction that are prohibited under international law, such as any propaganda for war and any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. To enforce this duty, States must prohibit by law information operations and activities amounting to such forms of speech.
4. States must refrain from engaging in, or supporting, any other information operation or activity that violates the rights of individuals within their jurisdiction, such as their right to life, health, private life, freedoms of thought and opinion, freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, right to vote and participate in public affairs.

5. States must take measures to protect the human rights of individuals within their jurisdiction from violation by information operations or activities carried out by other States and non-state actors. Where such protective measures interfere with human rights, they must be in accordance with applicable legal requirements, such as legitimate purpose, legality, necessity, proportionality and non-discrimination.

6. In regulating information operations and activities, States must not unduly restrict the right to freedom of expression and other rights guaranteed under international law.

7. In addressing the impact of information operations, States must ensure that information and technology companies are able to operate their services consistently with the human rights of their individual users.

8. The conduct of information operations or activities in armed conflict is subject to the applicable rules of international humanitarian law (IHL). These rules include, but are not limited to, the duty to respect and ensure respect for international humanitarian law, which entails a prohibition against encouraging violations of IHL; the duties to respect and to protect specific actors or objects, including medical personnel and facilities and humanitarian personnel and consignments; and other rules on the protection of persons who do not or no longer participate in hostilities, such as civilians and prisoners of war.

9. Conducting information operations or activities will amount to international crimes, such as genocide, including direct and public incitement thereto, war crimes and crimes against humanity, where the elements of those crimes are fulfilled.

10. The application of the aforementioned rules of international law is without prejudice to any and all other applicable rules of international law that provide protections against information operations or activities.
The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations

(Signatories: 124)

Reiterating the commitment expressed in the First, Second, Third and Fourth Oxford Statements to clarify rules of international law applicable in the use of information and communications technologies;

Noting that ransomware (i.e. malware designed to encrypt data and render it unavailable unless a demand is met) is a global threat, having been employed at an escalating pace by a growing number of malicious actors, including states and non-state groups for financial or political purposes, often connected to criminal and other unlawful activities such as terrorism, human and drug trafficking, money laundering, sanctions evasion, and the proliferation of weapons of mass destruction;

Stressing that the COVID-19 pandemic and our increased dependency on the Internet and other information and communications technologies have enhanced vulnerabilities to and opportunities for ransomware and other types of malware that facilitate its distribution, including the targeting of remote control or monitoring systems and the use of phishing emails, malicious websites or false notifications;

Considering that ransomware has, in the vast majority of cases where it has been employed, caused significant and widespread harm to public and private institutions, as well as individuals, such as financial loss, reputational damage, breach of confidentiality, and the significant disruption of critical infrastructure, including healthcare and education, while posing an imminent risk of destructive harm to industrial control systems such as electric grids, water distribution systems and nuclear power plants;

Bearing in mind that ransomware can take increasingly varied and sophisticated forms, including targeted and indiscriminate operations, and lead to the denial of access to and/or the unauthorized release of data if demands are not met;

We agree that:

1. Conduct carried out through information and communications technologies, such as ransomware operations, is regulated by international law.

2. States must refrain from conducting, directing, authorising or aiding and assisting ransomware operations which violate the principles of sovereignty or non-intervention in a state’s internal or external affairs, or amount to a prohibited threat or use of force within the meaning of the Charter of the United Nations. In particular, states must refrain from ransomware operations which are aimed at or result in disruption to electoral systems, healthcare, electric grids, water distribution systems, and nuclear power plants.

3. States must refrain from conducting, directing, authorising or aiding and assisting ransomware operations that result in violations of the human rights of individuals within their jurisdiction, such as the right to life, health, private life, education, property, freedoms of thought and opinion, freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds.

4. a) States must not allow their territory or infrastructure under their jurisdiction or control to be used by states or non-state actors for ransomware operations that are contrary to the rights of other states, when the former states know or should know of such operations.

b) To discharge those duties, states from which ransomware operation emanates, in full or in part, must take feasible measures to stop such operations and otherwise address the
situation. Such measures may include the conduct of investigations, the adoption of legal and technical measures, as well as cooperation with other states. Any measures taken in this regard must be compliant with applicable obligations under international law, including international human rights law.

5. States must take measures to protect the human rights of individuals within their jurisdiction from harmful ransomware operations, including when such operations are carried out by other states and non-state actors. To discharge this obligation, states may, among other measures, prohibit ransomware by law, take feasible steps to stop ransomware operations, mitigate their effects, investigate and punish those responsible, as well as prevent and suppress ransom payments to the extent possible. Where such protective measures interfere with other human rights, they must conform with applicable legal requirements, such as legitimate purpose, legality, necessity, proportionality and non-discrimination.

6. The use of ransomware during armed conflict is subject to the applicable rules of international humanitarian law (IHL). These rules include, but are not limited to, the duty to respect and ensure respect for IHL, which entails an obligation to prevent violations of IHL; the duties to respect and to protect specific actors or objects, including medical personnel and facilities and humanitarian personnel and consignments; the duties concerning objects indispensable to the survival of the civilian population as well as those concerning works and installations containing dangerous forces; and other rules on the protection of civilians, civilian objects, and of persons who no longer participate in hostilities, such as the sick, wounded, and prisoners of war.

7. The use of ransomware will amount to international crimes, such as genocide, war crimes and crimes against humanity, where the elements of those crimes are fulfilled.

8. The application of the aforementioned rules is without prejudice to any other applicable rules of international law that provide protections against ransomware and related activities.