Hacking Each Other to Death

Cyber-War and the Russia-Ukraine Conflict

Jean-François HENROTTE

Janice F. MULLIGAN

La guerre ne se déroule plus seulement sur le terrain, elle se joue dans le cyberespace. Aussi, nous plaidons pour l'adoption d'un protocole additionnel à la Convention de Genève pour tenir compte de cette nouvelle réalité. Bien sûr, le principe fondamental de l'effet utile des conventions internationales peut conduire à une condamnation des cybercrimes de guerre, mais un texte de droit positif réduirait l'incertitude juridique actuelle.

La guerra ya no se libra sólo sobre el terreno, se juega en el ciberespacio. Por ello, abogamos por la adopción de un protocolo adicional a la Convención de Ginebra que tenga en cuenta esta nueva realidad. Por supuesto, el principio fundamental del efecto útil de las convenciones internacionales puede llevar a una condena de los crímenes de ciberguerra, pero un texto de derecho positivo reduciría la actual inseguridad jurídica.

While pictures of bombed buildings and fleeing refugees circle the globe, digital war is less visible, but potentially just as deadly. The day the Russian invasion began, ViaSat (a satellite internet service) was affected by malicious software, crippling the Ukrainian army's communications. Banks' websites were made inaccessible, causing the spread of panic among Ukrainians.

Retaliation followed, when Anonymous (an army of civilian hackers) declared stealth cyberwar on Russia. Computer systems are now hacked by both sides, with not only denial of service attacks, but also with deception and disinformation rampant. A fake video of Vladimir Putin declaring peace with Ukraine caused chaos online, while another clip shows a deepfake of Volodymyr Zelensky surrendering to Russia.

The distinction between civilian and military can be blurred in a cyberwar. Distance from the battlefield is inconsequential. Experts typically condemn civilian hackers, but some make exception for the cyber-warriors aiding the Ukraine. Others view these civilian volunteers as active combatants, potentially unwittingly complicit in war crimes.

The Geneva Convention of 12 August 1949 (and its amendments) governs the conduct of war, but this body of law does not address cyberspace as a theater of conflict. The Convention sets out the fundamental principles of international humanitarian law: the principle of proportionality, the principle of military necessity, the principle of humanity, and the principle of distinction. Thus, under the Geneva Convention, war crimes are assessed based on proportionality (is the attack proportional to the threat); necessity of an attack, which entitles the parties to do the minimum necessary to obtain a military advantage; prohibition of unnecessary suffering, injury, and destruction; and the distinction between attacks on a military target as compared to a civilian one. In cyberwar, these criteria can be hard to discern.

A direct cyberattack on a hospital causing civilian casualties is a war crime, but what about taking out an electrical grid or the access to the internet that supplies a hospital and results in patient deaths from lack of needed medical treatment? The fundamental principle of the effectiveness of international conventions should lead us to interpret the Convention in this sense.

In February 2017, Brad Smith, Microsoft CEO, called for a "Digital Geneva Convention" to stem the flow of state cyber operations. Others believe a robustly developed international law already exists. Everyone agrees that enforcement will be a problem regardless of which bodies of law are referenced.

In 2021, NATO-sponsored legal experts began work on a project to determine the bounds of international cyber conflicts, which will culminate in the third edition

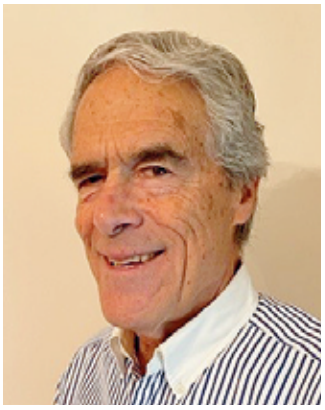
of the *Tallin Manual*, to be published in 2026. While the manual will not be legally binding, it will address issues such as which hacks are legally defensible and when it is appropriate to retaliate.

Treaties addressing cyberwar include the Budapest Convention on Cybercrime of 23 November 2001 (of which Russia is not a party, but even so proposed the adoption in 2021 of a United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes), and the pending African Union Convention on Cyber Security, as well as Personal Data Protection of 27 June 2014. Together with the Geneva Convention, these limited treaties, together with the *Tallin Manual*, provide guidance as to how existing international laws can be interpreted to fit cyber conflicts.

The time has come to regulate cyberspace. As Western sanctions mount against Russia and its oligarchs, the world holds its collective breath waiting for retaliatory cyberattacks to proliferate throughout the world.

If we are to avoid cyber-apocalypse, the time has come for international law to clearly and decisively address cyber weapons aimed at civilian populations. It will not be easy, but it is critical to world peace. ■

Jean-François HENROTTE
Lawyer, Lexing
UIA Director of Digital Strategy
Liege, Brussels
jf.henrotte@lexing.be
Janice F. MULLIGAN
Lawyer, Mulligan, Banham & Findley
President, UIA Health Law Commission
San Francisco, CA, USA
mulligan@janmulligan.com



Murray
S. LEVIN

Steven
M. RICHMAN

Sanctions: The United Nations, Russia, and Ukraine

Face à l'agression de la Russie contre l'Ukraine, qui comprend des actes pouvant être considérés comme un génocide, les auteurs ont examiné les recours possibles, offerts par le droit international et divers tribunaux de droit international, pour tenir la Russie responsable. L'enquête ne laisse pas beaucoup d'espoir quant à la possibilité de demander des comptes à la Russie dans ces scénarios.

Ante la agresión de Rusia contra Ucrania, que incluye actos que pueden considerarse genocidio, los autores consideraron los posibles recursos para responsabilizar a Rusia que ofrecen el derecho internacional y diversos tribunales de derecho internacional. El estudio no arroja muchas esperanzas de que Rusia rinda cuentas en esos supuestos.

The more relevant aspects of international law that are implicated by the Russian invasion of Ukraine are provided herein, with the bombing of children's hospitals and the apparent mass execution of civilians in Bucha, among other reported atrocities potentially implicate several aspects of international law. First, by these actions, Russia arguably has brought itself within Paragraph 139 of the 2005 World Summit Outcome Resolution A/60/L.1, which addresses the responsibility of the international community through the United Nations (UN) "to use appropriate diplomatic, humanitarian and other peaceful means" per the UN Charter "to help to protect populations from genocide, war crimes, ethnic cleansing and crimes against humanity." This UN resolution sets out the norm of the global "Responsibility to Protect (R2P)," which provides a basis for action of the Security Council. However, Russia's seat on the Security Council and veto power makes any hopes for enforcement of this resolution futile.