GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

ADDITIONAL NOTE TO THE NORM AGAINST OFFENSIVE CYBER OPERATIONS BY NON-STATE ACTORS

NORM

"Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur."

BACKGROUND

While information and communication technologies have positively transformed societies, they also pose new security challenges. The speed and ubiquity of cyber operations often poses considerable difficulties to states' judicial systems and international law enforcement cooperation. Despite these difficulties, it should be recalled that state sovereignty is the corner stone of the rules-based international system of peace and security. States have a monopoly on the legitimate use of force, strictly bound by international law. Some non-state actors, mainly private companies, advocate for the right to conduct offensive cyber operations across national borders, potentially claiming that it constitutes "self defense" as states do not have the capacity to adequately protect them against cyber threats. These non-state actors' offensive cyber operations are sometimes euphemistically referred to as "active cyber defense,"* including but not limited to so-called "hack-back," as they are conducted for defensive purposes.

Some states are unable to control—or chose to actively ignore—these practices, despite the risk they impose upon the stability and security of cyberspace. However, in most states such practices would be unlawful, if not criminalized, while in other states they appear to be neither prohibited nor explicitly authorized. A few states are, nevertheless, considering legitimizing non-state actors' offensive cyber operations. Indeed, some have decided or proposed legislation to allow offensive operations by non-state actors in their domestic legislation.

The Global Commission on the Stability of Cyberspace believes that these practices undermine the stability of cyberspace. They can result in serious disruption and damages, including for third parties, and are thus likely to trigger complex international legal disputes and escalate conflicts. States explicitly granting or knowingly allowing non-state actors the authorization to conduct offensive operations, for their own purposes or those of third parties, would set a dangerous precedent and would breach international law in most cases. The Commission believes that offensive measures should be reserved solely to states and recalls that international law establishes a strict and exclusive framework for international response to hostile acts that also applies to cyber operations. Similarly, under international law, non-state actors acting on behalf of states must be considered their agents and are therefore considered extensions of the state.†

If states permit such action, they may therefore be held responsible under international law.‡ States must act, domestically and internationally, to prevent offensive cyber operations by non-states actors.

* Active cyber defense should be understood as a set of measures ranging from self defense on the victim's network to destructive activity on the attacker's network. Offensive cyber operations within this continuum imply for the defender to act outside of its own network independently of their intention (offense or defense) and the legal qualification of their acts. Further work should be conducted on the definition of offensive cyber operations and active cyber defense.

† See "additional note" for a wider treatment of the case within international law.

ADDITIONAL NOTE

The Global Commission on the Stability of Cyberspace believes that offensive measures should be reserved solely to states and recalls that international law establishes a strict and exclusive framework for international response to hostile acts that also applies to cyber operations. As the UN GGE stated in its 2013 report, "[i]nternational law, and in particular the Charter of the United Nations, is applicable."[§] Occasionally, in responding to malicious cyber operations, states may decide to involve non-state actors to act on their behalf. In such cases, the acts of the non-state actors will generally be considered as the acts of the states pursuant to the legal criteria found in international law if these actors are exercising elements of governmental authority or acting on the instruction of, or under the direction or control of, the state as it has been codified by the International Law Commission of the United Nations in its 2001 Articles on the Responsibility of States for Internationally Wrongful Acts.

Non-state actors, acting on their own accord, should not undertake offensive cyber operations[¶] and states should prohibit such conducts in their domestic legislation. If a state grants such possibilities to a non-state actor, it may lead to a violation of its international obligations. This could occur either by virtue of a state amending its domestic legislation or on a case-by-case basis. In such a situation, a state is to be considered responsible—that is to say accountable—for allowing the conduct and may bear the obligation to provide reparations for the damage caused.

The Commission recalls the principle of due diligence under international law, which applicability in cyberspace has been recognized by the 2015 UN GGE report,[**] meaning that states are obliged not to knowingly allow their territories to be used for acts that are contrary to the rights of other states. In that sense, it should be noted that if a state permits non-state actors to undertake offensive cyber operations, the states where the consequences of the operations materialize may claim that the territorial state has breached its due diligence obligation. Indeed, the state victim of a cyber operation not attributable to another state but emanating from its territory may invoke its obligation of due diligence. In the same vein, the non-state actor's victim of cyber operations emanating from abroad, either from a state or a non-state actor, may ask their territorial state to invoke the obligation of due diligence of the state from the territory of which the cyber operations are conducted. If that state does not comply with its obligation of due diligence, and thus does not take the necessary but feasible measures to terminate the cyber operations, the territorial state of the victim may resort to proportionate and necessary countermeasures and measures of retorsion to incentivize the state to comply with its obligation of due diligence.

In addition to potentially being held legally responsible, a state permitting non-state actors to conduct offensive cyber operations as well as the acting non-state actors, may be held politically responsible by the international community and other actors, notably for weakening the international security and endangering the stability of cyberspace.

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

¶ Active cyber defense should be understood as a set of measures ranging from self defense on the victim's network to destructive activity on the attacker's network. Offensive operations within this continuum imply for the defender to act outside of its own network independently of its intention (offense or defense) and the legal qualification of its acts. Further work should be conducted on the definition of offensive operations and the various dimensions of active cyber defense.

** United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July 2015, A/70/174.