June 2nd, 2020


TLP White

This week, Hacking Healthcare takes a deeper look at international norms. Specifically, we will explain what international norms are, how they apply to cybersecurity and the healthcare sector, and why it is important for healthcare organizations to understand them. Welcome back to *Hacking Healthcare*.

1. **International Norms, Cybersecurity, and Healthcare:** The disturbing widespread acknowledgement of nation-state actors applying their considerable cyber capabilities to target the healthcare sector during the COVID-19 pandemic has poured fuel on the long running discussion of international cyber norms. While this discussion may often seem on the periphery of the cybersecurity discussions for healthcare organizations, these norms can have significant high-level impacts that trickle down to the day-to-day issues faced by the sector. The following is intended to provide a basic understanding of what international norms are, how they apply to healthcare and cybersecurity, and how better understanding this issue can inform long-term risk planning.

   **What are international norms?**

   To begin, we must define what international norms are. While there is no universally accepted definition, international norms are essentially actions or practices that are viewed by the entirety, or a large majority, of the international community as constituting normal accepted behavior by countries. It is also important to recognize that norms are not laws, international or otherwise, although their concepts may be written into or adopted as legally binding commitments.

   International norms can change over time to broadly reflect the global sentiment on international issues. Additionally, countries with great military and economic power, or diplomatic and cultural influence tend to exert disproportionate control on how norms are formed or evolve. Examples of international norms include those around nuclear nonproliferation, national sovereignty, and cybersecurity.

   International norms often develop as a method to create order and to establish mutually beneficial behaviors between members of the international community. They often develop collaboratively within international fora, such as the United Nations

("U.N.") but may also be championed by a particular country or group of countries that have a vested interest in an issue.

Regardless of how they are formed, becoming an established international norm requires the consensus of the international community to abide by what is agreed upon. This can lead to international norms being enshrined by certain countries in treaties, trade agreements, multilateral proclamations, and even within national laws.[1] Proponents of international norms believe that through their adoption, they can create a positive-sum solution (or partial solution) to a problem, even where enforceable legal commitments are not feasible.

**International norms in cybersecurity and healthcare**

It is important to recognize that cyber norms are in their relative infancy in comparison to longstanding international norms like national sovereignty, which is the concept that countries should not interfere in the internal matters and governance of other countries. This lack of maturation is embodied by an unsettled environment of many competing norms each promoted for different reasons by various countries and non-governmental entities.

One of the primary platforms where these cyber norms are debated is within the United Nations ("U.N.") Group of Governmental Experts ("GGE") and its parallel track the Open Ended Working Group ("OEWG"). Both groups represent multilateral approaches by states to develop and promote cyber norms under the umbrella of legitimacy that the U.N. provides.

The GGE is the better known of the two and represents a smaller group of countries (25) who tend to have more technical knowledge and influence in cyberspace than the OEWG, which is open to all member countries. The GGE is tasked with addressing cyber norms, principles, confidence building measures, as well as determining how international laws should apply in cyberspace.[2]

The GGE has been fraught with difficulties since its inception. The GGE process, which has ultimately created 6 working groups since 2004, didn't begin to have some measure of success until 2010. In the following years, participants came together on a consensus over the growing risk in cyberspace and the general applicability of international laws. This culminated in 2015, with the issuance of a report that outlined 11 norms, principles, and guiding statements for cyberspace.[3, 4] However, by 2017, differences between countries involved, specifically the United States, Russia, and China all but halted the GGE process.

Despite the stop-start nature of the U.N. processes, they have contributed greatly to where things stand today. Below are three cyber norms that were influenced by those processes, have gained traction in recent years, and directly affect the healthcare sector.

- **Critical Infrastructure** – The international community broadly believes that attacking critical infrastructure is deemed unacceptable behavior. While countries may have differences of opinion in what qualifies as critical infrastructure, the U.N. OEWG insists all nations, especially during COVID-19, consider healthcare a critical infrastructure sector.[5]

- **Industrial Espionage** – The international community broadly believes that countries using their national cyber capabilities for industrial espionage, or knowingly allowing non-state actors to conduct such activities within its territory, is unacceptable behavior.[6] This could include data related to healthcare devices, treatments, and research.

- **Active Cyber Defense / "Hack Back"** – While less a settled matter compared to the other two, the current consensus does not support organizations taking initiative with offensive measures in response to cyber-attacks.[7] While few private sector organizations are currently in a position to undertake effective active cyber defense, it is nevertheless important to establish appropriate behavior to avoid potential mis-identification and escalation that could lead to broader conflict.

Even though all of these norms were generally developed and agreed upon by governments in international institutions, they clearly have impacts on the daily operations of healthcare cybersecurity. The International condemnation of the cyberattacks and intelligence gathering operations perpetrated against healthcare entities during COVID-19 is a result of the flagrant disregard for the first two cyber norms illustrated above. Additionally, a disinclination in global support for the third has constrained the type of retaliatory action that could impose costs on conducting such attacks. While these three prominent cyber norms directly affect the healthcare sector, there are dozens of others that affect it.

*Analysis & Action*

*H-ISAC Membership Required*

## *Congress –*

Tuesday, June 2nd:

- House - Committee on Energy and Commerce - Hearing: "On the Front Lines: How Governors are Battling the COVID-19 Pandemic"

June 2nd, 2020

Wednesday, June 3rd:
- Senate – Committee on Commerce, Science, and Transportation – Hearing: "to examine the state of transportation and critical infrastructure, focusing on the impact of the COVID-19 pandemic"

Thursday, June 4th:
- House - Committee on Appropriations - Subcommittee on the Departments of Labor, Health and Human Services, Education, and Related Agencies - Hearing: "COVID-19 Response"

## *International Hearings/Meetings –*

***EU –*** - No relevant hearings

## *Conferences, Webinars, and Summits –*

--Identity for the CISO – Becoming 'Identity-Centric' – Webinar (6/3/2020)
https://h-isac.org/hisacevents/identity-for-the-ciso/
-- An H-ISAC Framework for CISOs to Manage Identity – Webinar (6/10/2020)
https://h-isac.org/hisacevents/framework-for-cisos-to-manage-identity/
-- Life as a CISO by Axonius – Webinar (6/11/2020)
https://h-isac.org/hisacevents/life-as-a-ciso-axonius/
-- Securing the IoT Threat in Healthcare by Palo Alto Networks – Webinar (6/24/2020)
https://h-isac.org/hisacevents/palo-alto-networks-navigator-webinar/
H-ISAC Monthly Member Threat Briefing – Webinar (6/30/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-9/
--Healthcare Cybersecurity Forum - Mid-Atlantic – Philadelphia, PA (7/17/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426497
--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--H-ISAC Security Workshop - Greenwood Village, CO (9/16/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-greenwood-villiage-co/
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--H-ISAC Cyber Threat Intel Training - Titusville, FL (9/22/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-titusville-fl/
--H-ISAC Security Workshop - Forchheim, Germany
https://h-isac.org/hisacevents/h-isac-security-workshop-forchheim-germany/
--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)
https://h-isac.org/hisacevents/summit-on-security-third-party-risk/
--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--CYSEC 2020 – Dubrovnik, Croatia (10/27/2020 – 10/28/2020)
https://h-isac.org/hisacevents/cysec-2020-croatia/
--H-ISAC Security Workshop - Mounds View, MN (10/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny/

--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--H-ISAC Security Workshop - Seattle, WA – (10/29/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-seattle-wa-2/
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/
--H-ISAC Security Workshop - Paris, France (11/18/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-paris-france/

## *Sundries –*

***-- Japanese IT services firm reveals hack affecting up to 621 corporate customers***
https://www.cyberscoop.com/ntt-hack-japan-customer-data/

***-- Apple fixes bug that could have given hackers full access to user accounts***
https://arstechnica.com/information-technology/2020/06/apple-fixes-bug-that-could-have-given-hackers-unauthorized-to-user-accounts/

***-- An advanced and unconventional hack is targeting industrial firms***
https://arstechnica.com/information-technology/2020/05/an-advanced-and-unconventional-hack-is-targeting-industrial-firms/

## Contact us: follow @HealthISAC, and email at contact@h-isac.org

---

[1] https://carnegieendowment.org/publications/interactive/cybernorms
[2] https://dig.watch/processes/un-gge#:~:text=The%20United%20Nations%20Group%20of,group%20in%20the%20field%20of
[3] https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[4] https://carnegieendowment.org/files/Cyberspace_and_Geopolitics.pdf
[5] https://www.dfat.gov.au/sites/default/files/joint-oewg-proposal-protection-health-infrastructure.pdf
[6] https://www.jstor.org/stable/resrep10473?seq=1#metadata_info_tab_contents
[7] https://www.technologyreview.com/2019/06/21/134840/cybersecurity-hackers-hacking-back-us-congress/