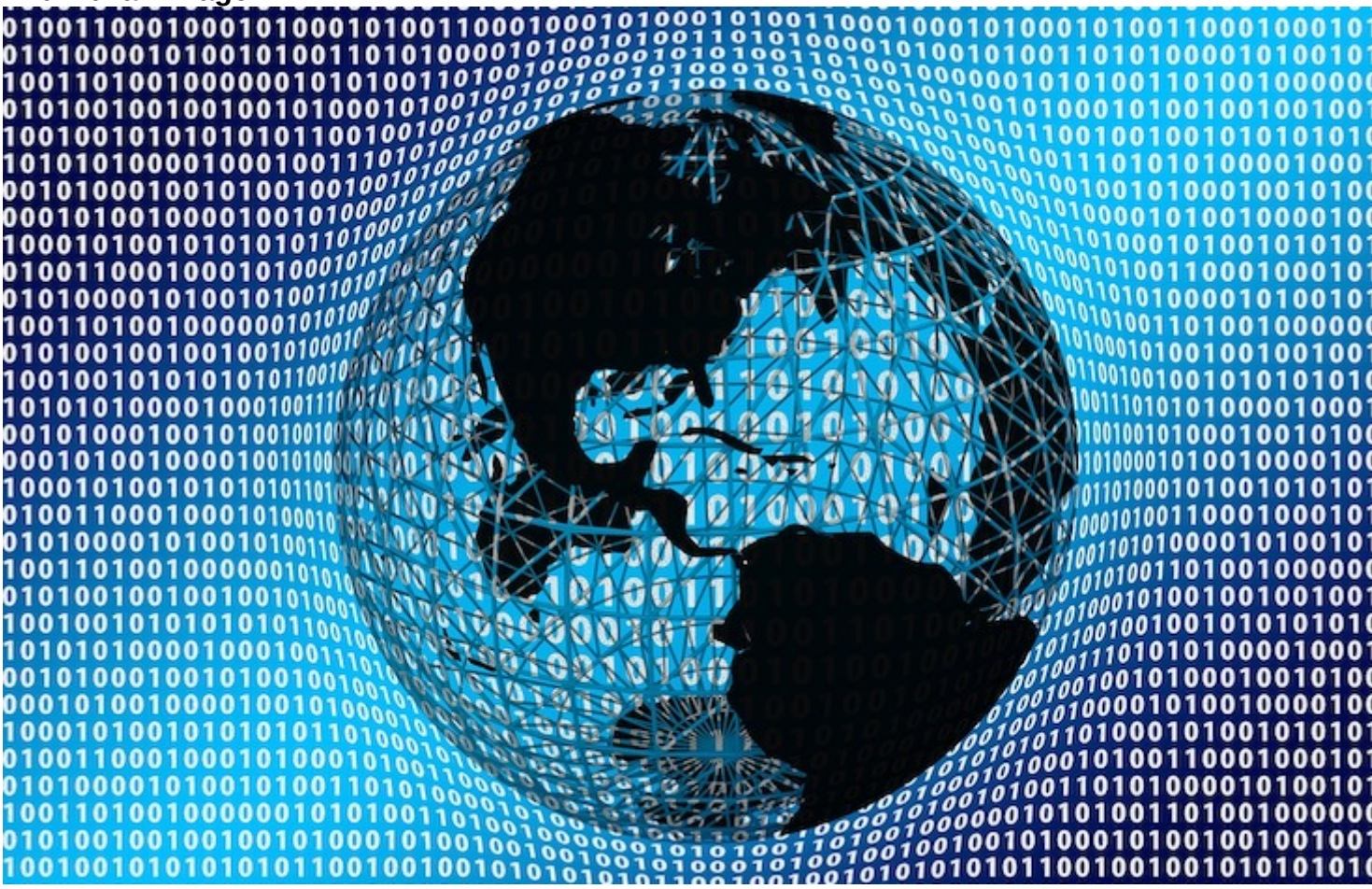
Published on *USC Center on Public Diplomacy* (https://uscpublicdiplomacy.org)

Thumbnail Image:



May 29, 2019 by Soft Power 30

Global collision or collaboration? Addressing a framework for cyber policy [1]

Picture the images that run through your head when you read about cyber security or hear about cyber threats and resilience. The phrases conjure images of engineers frantically translating number sets into increasingly self-sufficient machines, dark rooms in which hackers assisted by a multitude of inhuman bots and trolls craft sinister plots against an unassuming public and bewildered policymakers just hoping their teams behind the screens can find a patch, sort a solution, reassure the public that everything is under control. These images are intangible. They are mysterious. They are secretive and they are scary.

For a small but growing community of experts dedicated to building an international framework for addressing cyber policy, attributing cyber-attacks and building public and private sector momentum around prioritizing cyber security, the image is part of the problem. In a world where the conversation around the governance of cyber policy is one of the most relevant and urgent challenges of our time, the first step we must take to establish a global

framework around it is to take a step away from the world of computer science and dive straight into the realm of communications to change the narrative—to widen the spectrum of actors who are involved in this debate.

Cyber vulnerabilities operate in reverse of traditional defense vulnerabilities. While in the fields of nuclear power, highly-trained Special Forces, elaborately-armored tanks and aircraft carriers, we are only as strong as the most powerful and most robust amongst allies; in the realm of cyber security we are only as strong as the weakest link. Indeed, 80 percent of cyber security breakdowns are attributable to the simplest vulnerabilities, not the most sophisticated actors.

Addressing this realization leads us into one of the most critical realities in creating the right global framework for cyber policy. While it's tempting to address cyber policy in the context of defense, a template based on military and weapons mobilization fails to provide the appropriate prototype. A far more relevant model comes, for example, from the world of global health. Pandemics, like cyber breaches, evolve as they spread across populations. While the missile strikes a specific, targeted geographical area, a disease spreads through complex exposures involving global travel and trade, similar to cyber-attacks impacting vulnerable systems without necessarily having geographic specification or limitation.

Re-framing the conversation around how we describe cyber challenges is also essential to opening a robust, transparent global dialogue.

Equally, algorithmic solutions for addressing cyber-attacks are frequently drawn from models based on global health systems. A public trained to vaccinate as part of their yearly routines is a public readily able to translate this defense mechanism to health check-ups in their digital lives, taken as seriously as the flu. Establishing fresh narratives around cyber security by moving the global conversation around cyber policy beyond the realm of defense is a necessary first step in identifying and deploying a strategy that will work long-term.

Re-framing the conversation around how we describe cyber challenges is also essential to opening a robust, transparent global dialogue. When cyber security is intrinsically linked in the government and citizen mindset to covert operations and military weapons systems, it is consistently over-classified. Indeed, experts agree that until we establish a better ecosystem around addressing and attributing cyber-attacks, we will fall into a pattern of classification as default as opposed to transparency as default. The result is a chronic failure in the global community to respond appropriately to cyber threats—or even understand them.

We must take a page from the playbook of, for example, the airline industry, which took transparency as its default approach. Because operational failures in the airline industry are openly available and analyzed, the culture within the industry is one of sharing more than it is one of secrecy. Cyber security is currently stuck in a cyclical pattern of secrecy, which in turn creates a culture whereby attacks are covered up as long as possible so as not to give a vulnerable impression to the voting public or to anxious shareholders. At both the state and the company levels, we must make a concerted effort to step up to the plate in establishing openness in dialogue and transparency as a default response. While initially this might

introduce some shock to the ecosystem, long-term it will build trust.

The time is now to establish a playbook for the global governance of cyber policy. In truth, the time was yesterday...

The time is now to establish a playbook for the global governance of cyber policy. In truth, the time was yesterday, but in highly innovative environments risks are not weighed equal to opportunity, and the tendency to place faith in the market's ability to reward problem-solving sometimes results in under-investment in issues that would otherwise receive strict attention. While some experts today worry that a strong framework for cyber policy will not take shape until cyber has its "9/11 moment," many agree that with the right global commitment and investment, we can build momentum before a crisis escalates beyond our ability to effectively respond.

We must ask influencers within the technology sector to serve as ambassadors for cyber health, encouraging the public to "vaccinate" themselves to build resilience. We must galvanize tech philanthropists to get involved in funding the research and multi-stakeholder harm observatories that will lead the way in the sharing of information, transparency of attack and united effort towards response. We must enlist the most qualified communications experts to craft narratives that bring cyber policy out of the shadows and into an approachable national and international dialogue. And at every step along the way, we must involve government, corporate, technologists and civil society leaders to ensure that our approach to global cyber policy is, indeed, global.

These networks—representative of the public/private partnerships that are absolutely necessary in any pivotal moment of global concern—are vital to introduce a cohesive, well-respected global governance and response framework. Building these networks and making transparency their default approach, will take trust and the judicious application of soft power. At a time when the majority of people coming online in some of the world's most-populous countries will not speak English, and when some of the countries with strongest expertise in this space do not share democratic principles as the core driver behind cyber security, we cannot disassociate cyber policy from human rights, freedom of expression and quality of an informed life.

What is more, the trade-offs between transparency and privacy, between cyber security and public safety and between public sector, private sector and individual responsibilities need to be more vocally socialized. As the 21st century marches on, technology has changed the ways in which nations and their citizens are empowered. And so the future of cyber policy is emblematic of the values our connected technologies both enable and threaten. Getting this right will not only create a more secure world, but also a fairer, more just one in which the creativity of the many wins out to the power of the few.

Note from the CPD Blog Manager: *This piece, written by Elizabeth Linder, originally appeared in the 2018 Soft Power 30 report.*

Elizabeth Linder founded the Conversational Century in 2016 and serves as Chair of the Kinross House Meetings in Scotland. She is a Senior Consulting Fellow at Chatham House and Executive Director of Global Communications & External Affairs at Beautiful Destinations.