# Submission: Mallory Knodel, ARTICLE 19; Matthew Shears, Global Partners Digital

2018 IGF Best Practices Forum on Cybersecurity

*On behalf of a group of experts in human rights and cybersecurity incubated by the Freedom Online Coalition working group "An Internet Free and Secure" from 2013-2017, our submission aims to highlight that individual security is a core purpose of cybersecurity and a secure Internet is central to human rights protection in the digital context. Recognition of this mutuality is essential to understanding that cybersecurity norms must ultimately serve all Internet users and in particular human rights defenders, journalists, activists and disadvantaged populations. We have chosen to respond to questions 1, 2, 3 and 6.*

## 1. How do you define a culture of cybersecurity?

Cybersecurity and human rights are complementary, mutually reinforcing and interdependent. Both need to be pursued together to effectively promote freedom and security. Recognizing that individual security is at the core of cybersecurity means that protection for human rights should be at the center of cybersecurity policy development. Such an approach is instrumental in reminding policy-makers that cybersecurity must take into account individual security and human rights and that, as a consequence, cybersecurity policies should be human rights respecting by design.

Yet, in the public debate about how to provide security in the digital context, the dominant narrative has become increasingly entrenched pitting privacy and other human rights against public safety and national security. In practice, though, threats to privacy and other human rights can also harm public safety and security. This binary framing is therefore damaging to both sides of the equation, and creates antagonisms where mutual reinforcement is possible. Framing privacy and other human rights as antithetical to public safety and national security is not only misleading, but undermines public safety and security, as well as freedom. Raising the profile of human rights protections in existing cybersecurity policy-making is necessary to offset this trend.

In the context of increasing cyber vulnerability, where cybersecurity and cybercrime challenges are increasing in frequency and complexity, there is a need for all stakeholders to work together to preserve human rights, particularly privacy and free expression. Individual security is a core purpose of cybersecurity and a secure Internet is central to human rights protection in the digital context. We use the following definition of cybersecurity to reinforce that notion that privacy and confidentiality of information are essential to the security of people, as well as to data, especially in the digital context where physical security and digital information

are linked:

> *International human rights law and international humanitarian law apply online and well as offline. Cybersecurity must protect technological innovation and the exercise of human rights.*
>
> Cybersecurity is the preservation – through policy, technology, and education – of the availability*, confidentiality* and integrity* of information and its underlying infrastructure so as to enhance the security of persons both online and offline.

# 2. What are typical values and norms that are important to you or your constituents?

As a result of the four-year initiative of the FOC working group, we produced the following policy recommendations, which were endorsed by all 30 state members of the FOC. These recommendations are a first step towards ensuring that cybersecurity policies and practices are based upon and fully consistent with human rights – effectively, that cybersecurity policies and practices are rights-respecting by design.

1. Cybersecurity policies and decision-making processes should protect and respect human rights.
2. The development of cybersecurity-related laws, policies, and practices should from their inception be human rights respecting by design.
3. Cybersecurity-related laws, policies and practices should enhance the security of persons online and offline, taking into consideration the disproportionate threats faced by individuals and groups at risk.
4. The development and implementation of cybersecurity-related laws, policies and practices should be consistent with international law, including international human rights law and international humanitarian law.
5. Cybersecurity-related laws, policies and practices should not be used as a pretext to violate human rights, especially free expression, association, assembly, and privacy.
6. Responses to cyber incidents should not violate human rights.
7. Cybersecurity-related laws, policies and practices should uphold and protect the stability and security of the Internet, and should not undermine the integrity of infrastructure, hardware, software and services.
8. Cybersecurity-related laws, policies and practices should reflect the key role of encryption and anonymity in enabling the exercise of human rights, especially free expression, association, assembly, and privacy.
9. Cybersecurity-related laws, policies and practices should not impede technological developments that contribute to the protection of human rights.
10. Cybersecurity-related laws, policies, and practices at national, regional and international levels should be developed through open, inclusive, and transparent approaches that involve all stakeholders.
11. Stakeholders should promote education, digital literacy, and technical and legal training as a means to improving cybersecurity and the realization of human rights.

12. Human rights respecting cybersecurity best practices should be shared and promoted among all stakeholders.
13. Cybersecurity capacity building has an important role in enhancing the security of persons both online and offline; such efforts should promote human rights respecting approaches to cybersecurity.

# 3. Within your field of work, do you see organizations stand up and promote specific cybersecurity norms? This can be either norms at an inter-state level, or norms that only apply within your community or sector.

Support for rights respecting cybersecurity norms can be found here: https://freeandsecure.online/supporters

The following publications have cited our normative framework, and the policy recommendations in particular:

- Mackinnon, Rebecca, Andi Wilson and Liz Woolery. *Internet Freedom at a Crossroads. Recommendations for the 45th President's Internet Freedom Agenda.* New America's Open Technology Institute, December 2016, https://na-production.s3.amazonaws.com/documents/Internet__Freedom_Agenda_12_21.pdf
- Sequera, Maricarmen, Amalia Toledo and Leandro Ucciferri. *Derechos Humanos y Seguridad Digital: Una Pareja Perfecta.* January 2018, https://www.tedic.org/wp-content/uploads/sites/4/2018/03/InformeCiberseguridadParte1.pdf
- Del Campo, Agustina. *Towards an Internet Free of Censorship II. Perspectives in Latin America.* Universidad de Palermo, CELE. http://cyberlaw.stanford.edu/files/publication/files/Towards_an_Internet_Free_of_Censorship_II_10-03_FINAL.pdf
- Marda, Vidushi and Stefania Milan. *Wisdom of the Crowd: Multistakeholder Perspectives on the Fake News Debate*. Internet Policy Review series, Annenberg School of Communication, May 2018, https://ssrn.com/abstract=3184458
- Finnemore, Martha, Duncan B. Hollis. "Constructing Norms for Global Cybersecurity." *American Journal of International Law*, 110(3), July 2016, pp. 425-479. https://doi.org/10.1017/S0002930000016894
- SOUZA SOBRINHO, P. C. G. de. *A segurança cibernética: uma abordagem securitizadora e a ascensão de um regime internacional*. Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, João Pessoa, 2017. http://dspace.bc.uepb.edu.br/jspui/handle/123456789/14563
- Testart Pacheco, Cecilia Andrea. *Understanding the institutional landscape of cyber security.* Massachusetts Institute of Technology, 2016, https://dspace.mit.edu/handle/1721.1/104820

# 6. What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?

The following are required of a global or regional initiative to implement such norms and standards:

1. A fundamental rethink of the dominant rights versus security paradigm and recognition that human rights and cybersecurity are mutually reinforcing and interdependent
2. Sustained and deep engagement in international policy and in particular cybersecurity dialogues at key international forums to promote such norms.
3. Case study development demonstrating the beneficial effects of people centric cybersecurity policy.
4. Consistent evaluation of cybersecurity policies and strategies using a human security framework, such as indicators based on the above norms.
5. Multi-stakeholder initiatives that combine these elements are an absolute necessity.