Remarks on the value of multistakeholder engagement: the lessons from the Ransomware Task Force

Delivered at EU delegation to the UN on the margins of the OEWG meeting

Megan Stifel
Chief Strategy Officer, Institute for Security and Technology

Jul 27, 2022

Thank you for asking me to come to speak about how the multistakeholder community can help address issues of peace and security in cyberspace. I've been invited to speak on the "multistakeholder contribution to norms" and will talk about how the Ransomware Task Force took a multistakeholder approach in developing its framework for combating ransomware, which it published in April 2021.

Let me start by describing what the Ransomware Task Force (RTF) was, what our key recommendations were, and how we've continued to move forward with implementing and advocating for those recommendations.

More than 60 members, including from software companies, government agencies, cybersecurity vendors, financial services companies, nonprofits, and academic institutions formed the RTF. The group included really broad participation - we had participants from local government, such as officials from Jefferson County, Colorado, representatives from not-for-profit entities, and large multinational corporations like Amazon Web Services. We also welcomed participation from outside the United States, including government partners, industry partners such as CFC Underwriting from the United Kingdom, and the Cyber Peace Institute, which is headquartered in Geneva.

Many of the specific recommendations in the Ransomware Report were focused on the United States context, and we're currently working on interpreting the recommendations to other contexts and engaging with partners to implement them in other national contexts.

The breadth of the participants reflects the reality that ransomware victims include the for-profit, not-for-profit, and government sectors. This is a multistakeholder problem, and solving it requires input from the multistakeholder community. Only by hearing from those entities impacted by ransomware could we think about how to make progress to address solutions.

The Ransomware Report outlines four topline goals to address ransomware, each of which has specific recommendations:

1. Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy
2. Disrupt the ransomware business model and decrease profits
3. Help organizations prepare for ransomware attacks
4. Respond to ransomware attacks more effectively

I should note that in the Ransomware Report we use the term "attack" not to mean an armed attack under international law, but rather an incident of ransomware by a malicious or criminal actor. That is particularly important as we are talking about issues of peace and security between states.
These recommended goals are in line with the framework of responsible state behavior in cyberspace, demonstrating how the multistakeholder community can help affirm that framework, and assist states in implementing it.

For the purposes of connecting to the existing norms of responsible state behavior in cyberspace, most of these recommendations are relevant to a number of the norms. Three that jump out at me as most relevant are 13(g) and 13(h), which relate to protecting critical infrastructure, and 13(d), regarding cooperating to combat criminal use of information and communication technology (ICTs).

The norm that "States should take appropriate measures to protect their critical infrastructure from ICT threats" [13(g)] is really a guiding principle of the effort we were undertaking, which is to say helping to outline key steps that states could take to mitigate ransomware-specific harm. By providing these recommendations with a multistakeholder imprimatur, and by bringing private sector resources and attention to the problem, the Task Force was able to help the government to do this work as effectively as possible. By doing it transparently, we also helped other states to understand our goals and objectives, increasing predictability and setting the stage for clear state-to-state communications.

In addition to states taking measures domestically, norm 13(h) reads, "States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty."

As articulated in the RTF, there is a critical need for states to live up to this norm. The original Ransomware Report articulated the importance of using both carrots and sticks to incentivize states to take action when there are malicious activities emanating from their territory, and there has been definite, though somewhat unsustained, progress on this.

Our intent in calling for this was to lend weight to the need for diplomatic action, to demonstrate the importance that the technical community and the private sector place on addressing this not only as a technical issue, but as a national security issue and something that implicates peace and security.

And finally, norm 13(d), the norm that "States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats."

As the Ransomware Report makes clear, an effective response to criminal ransomware activity requires states to follow through on this norm, by taking action within their own national policy and legislation, as well as through building mechanisms for collaboration with one another.

For example, in the Ransomware Report, we highlighted the importance of working with law enforcement attachés in U.S. embassies to partner with their host government counterparts to investigate and prosecute perpetrators of ransomware attacks. European and U.S. officials have made a lot of progress in that effort, with criminals that had been operating with impunity arrested in multiple European countries, most significantly in Russia.

There is a lot more to be done in this effort, including things like standard templates for reporting ransomware incidents, and increasing capacity building to states that have the desire but not the capacity to take these actions. The multistakeholder community can shape that effort to make it as effective as possible for victims and law enforcement alike. Because so much of the information about attacks is held by the private sector, it's critical that information sharing processes include private sector input.

So, just to sum it up, the RTF used our multistakeholder bully pulpit to underscore the reality that we can't address this without action by states to address it with all stakeholders.

We've certainly seen some progress in implementing the recommendations of the Ransomware Report, and I encourage you to look at our May 2022 report highlighting areas of progress and areas needing additional attention.

Attachments

The Ransomware Task Force Report, April 2021:
https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf

The Ransomware Task Force Progress Report, May 2022:
https://securityandtechnology.org/wp-content/uploads/2022/05/rtf-progress-report-may22-1.pdf

The Blueprint for Ransomware Defense, August 2022:
https://securityandtechnology.org/wp-content/uploads/2022/08/IST-Blueprint-for-Ransomware-Defense.pdf