ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 05/25 (May) – Special Edition Op-Ed

# The Case for Greater Visibility and Use of the United Nations Norms of Responsible State Behavior in Cyberspace to Bolster Accountability and Stability

*by Chris Painter, former President of the Global Forum on Cyber Expertise and a founding principal of the Cyber Policy Group*

1. Nearly a decade ago, despite wide geopolitical differences, a group of governmental experts in the United Nations (U.N.), including the United States, Russia and China among others, reached a remarkable consensus on a set of norms of responsible behavior for nation states in cyberspace (Figure 1). Subsequently, every country in the U.N. endorsed these norms as part of a broader stability framework for cyberspace that also includes the application of existing international law in cyberspace, and the articulation and use of confidence and transparency measures designed to avoid the inadvertent escalation of cyber conflict.

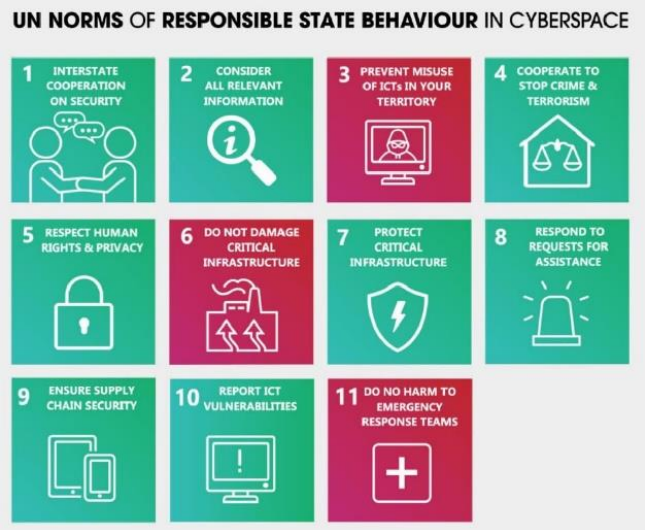


*Figure 1: 11 U.N. Norms of Responsible State Behavior in Cyberspace (Source: Australian Strategic Policy Institute)*

2. The eleven agreed upon norms, or rules of the road, are comprised of both "norms of restraint", such as not attacking a country's critical infrastructure using cyber means in peacetime, and norms of cooperation, such as an expectation that states will cooperate in mitigating malicious cyber activities coming from within their borders. Although the norms are expressly voluntary and non-binding, they nevertheless are important political commitments by every state and form a powerful basis for calling out any lack of adherence to the norms and as a basis for both other countries and nonstate stakeholders to take action to hold transgressors accountable.

3. In addition, the agreement on norms, as well as the larger cyber stability framework, serves as an important counter to the oft prevailing view that cyberspace is a lawless and ungoverned domain – particularly when states are the aggressors. This is particularly important as nation state attacks on critical infrastructure are ever increasing and militaries around the world are building or employing cyber offensive capabilities. Not surprisingly, given the increasing threat, the norms and larger stability framework has been endorsed again and again in the U.N. by countries across the geopolitical spectrum.

4. Yet, with some few important exceptions, the U.N. cyber norms are largely unknown outside the denizens of U.N. diplomats and international lawyers. There is little awareness or use of the norms on a political level in countries and many militaries seem similarly unaware of their precepts despite the fact that the norms were designed, in part, to help govern their activities. This lack of mainstreaming of the norms on a political and military level clearly limits their effectiveness in achieving greater accountability for bad actions and achieving cyber stability. Even within the U.N., ongoing and seemingly intractable debates on the necessity of a binding cybersecurity treaty, led by Russia and China but opposed by most Western states, and whether there needs to be additional norms or whether the focus should be on the implementation of existing agreed norms, have become geopolitical divides limiting the practical and political application of the existing normative framework.

5. This is unfortunate as cyber-attacks by nation states that seemingly violate agreed norms have risen substantially both in number and severity – affecting states and disrupting businesses and society as a whole. The Russian-sponsored NotPetya worm produced widespread effects including temporarily crippling Maersk's global shipping operation while the North Korean WannaCry worm took down the U.K.'s National Health Care system – both apparent attacks on critical infrastructure. Further, malicious ransomware groups operate with impunity from the borders of countries that shield them, despite a norm of "due diligence" and cooperation to stemming such criminal threats. States have taken

some actions like collective attribution of serious disruptive cyber events though the actual text or fact of the agreed-on norms being violated is seldom cited – particularly at a leader or political level. Some in the private sector and civil society have called out norm violations but that has been more the exception than the rule. If the norms are to be more than nice words on paper and actually have an effect in shaping behavior and accountability, they need more mainstream exposure and implementation.

6. Some important steps have already been taken in this direction that can serve as the foundation for further action. In 2018, ASEAN Ministers responsible for cybersecurity and leaders endorsed the UN norms and made a commitment to operationalize the norms to promote regional stability. Bucking the general trend of high-level political attribution ignoring the norms, the High-Level Representative for the EU External Action Service has cited the norms in calling out malicious state attacks on infrastructure and democratic processes. Malaysia and Singapore have championed a practical Norms Implementation Checklist in the U.N. that helps break through the theoretical debates in that body and makes the norms more understood, operationalized and accessible.

7. But more can be done. The first step is to build greater awareness of the norms and what they mean particularly at the political level of governments, within the military and with the private sector and civil society. If there is a better understanding of the political commitments their countries have made, the military in particular can better use the norms as appropriate guideposts as they attain greater cyber capabilities and build military doctrine around these issues. This is especially true of norms of restraint that take certain potential targets generally off the table – like civilian critical infrastructure or computer emergency response teams. The second is for governments – particularly at a political level – to better reference the norms as important commitments with consequences when they are blatantly violated. Though ensuring accountability for, and mounting a collective response to, malicious state cyber activity is complicated, and might involve a range of economic, diplomatic and even military actions, they are all made stronger by a collective recognition that a state has transgressed a norm of responsible state behavior they have expressly endorsed as a basis for any responsive action or statement.

8. Private sector and civil society groups should also be able, when appropriate, to call out violations of norms and detail how such violations affect them – particularly as they bear the brunt of attacks on critical infrastructure that they operate and depend upon. That activity can go a long way to making the real-world consequences of norm violations, and cyberattacks more generally, more understood by the public at large. It is also important for the media to better report on disruptive incidents in the context of these norms, making it clear that political

commitments have meaning and encouraging governments to ensure that appropriate actions are taken to achieve the goal they set of a stable and prosperous cyberspace.

9. Of course, mainstreaming the norm conversation is no simple task and will require the attention and leadership of a number of governments, regional organizations, the private sector, civil society and a range of other actors. And awareness of, complying with, and taking action against violation of the norms of responsible state behavior is only one piece of the larger puzzle of attaining a stable and peaceful cyberspace that includes, among other things, building better resilience, cyber defenses, response capabilities and governance. Yet given the rising threats in cyberspace and our increasing reliance on computer networks, creating more understanding of responsible state behavior and building collective action to ensure compliance by those who would violate those precepts cannot be put on hold.

**The views expressed in this Cyber Digest are that of Christopher Painter, a member of ACICE's Experts Panel. Painter has been on the vanguard of cyber issues for over thirty years, serving in the U.S. government as a cybercrime prosecutor, a senior official at the Department of Justice, White House National Security Council and as the first dedicated cyber diplomat in the State Department. Since leaving government service Painter has served as the President of the Global Forum on Cyber Expertise and is currently a founding principal of the Cyber Policy Group.*

# Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
**ADMM Cybersecurity and Information Centre of Excellence**

• • • • •