Compliance & Capacity Skills
International, LLC

Sanctions Practitioners
Compliance Trainers

Circumventing Sanctions - an Overview of Technological Threats

Presentation to Panel Discussion on
UN Sanctions and Digital Technologies: Threats and Opportunities
9 February 2016

Digital technologies in their evolving applications are used to convey life-saving or peace-making information, to educate, assist in global communication, commerce or science, in the delivery of aid, and to facilitate public and private sector governance, among many other important tasks. It is hard to imagine a world without Internet, mobile and satellite telecommunications or social networks. Yet, because no universal defense of these networks or global norms for the comportment of users exists, incalculable losses are a very real risk. This lack threatens to turn digital technologies from an essential humanitarian infrastructure into a profound threat to international peace and security.

The following table illustrates widely reported types of threats to national and international peace and security.

I. Threats in the context of cyber-warfare
Cyber attacks against critical infrastructures or command and control centers
Cyber attacks to undermine the global financial system

II. Threats that support sanctions violations
Use of the Internet to circumvent sanctions and related national laws
Utilizing internet services for command and control functions
Acquisition of conventional arms
Acquisition of WMD material
Transmission of WMD-relevant knowledge
Fabrication of false end-use certification
Enlisting of services to transport embargoed arms or goods
Enlisting of services to finance transactions involving embargoed arms or goods
Use of crypto-currencies
Recruitment of combatants
Recruitment of children into war
Commercialization of conflict minerals
Commercialization of wildlife and wildlife products
Disseminating and enabling hate-speech or hate-crimes

How can states intervene in a meaningful manner, in particular through the Security Council's mechanisms to thwart such threats?

Leaving aside questions related to the waging of cyber warfare, we propose to focus on two possible practical approaches: things we should do now, and things we should do to secure the future.

Possible immediate measures

It is well established that militias, terrorists or WMD proliferators regularly use digital technologies to further their various forms of sanctions violations. It is equally well established that international media and consulting firms defend against the potential reputational damage that might result from providing assistance to such perpetrators by building and offering to other industries massive compliance data-base tools. Both trends started about 15 years ago. The first UN expert group published findings about UNITA’s abuse of the Internet (see the Angola Monitoring Team reports S/2001/363 and S/2001/966) and subsequent expert groups reported how Somali militias utilize the Internet to incite clan members to violence; how Congolese and Sudanese militias use email and satellite communication to acquire arms or as a command and control tool, and most importantly for the international community, how Al Qaida, ISIS/ISIL and their regional affiliates employ the Internet for a wide range of tasks.

Particularly responding to ISIS / ISIL, the last three Council resolutions have spelled out specific measures against the "financing, arming, planning, or recruiting for terrorist organizations ... or otherwise supporting their acts or activities, including through information and communications technologies, such as the internet, social media, or any other means" (Res. 2214 (2015).

While these terrorism-related provisions are certainly welcome, they are no substitute for a global norm that could leverage sanctions against all types of threats to international peace and security, as table 2 illustrates.

Applicability of current sanctions measures
(contingent on potential targets acting for Al-Qaida/ISIL)

I. Threats in the form of attacks	
Cyber attacks against critical infrastructures or command and control centers	
Cyber attacks to undermine the global financial system	
II. Threats that support sanctions violations	
Use of the Internet to circumvent sanctions and related national laws	✓
Utilizing internet services for command and control functions	✓
Acquisition of conventional arms	✓
Acquisition of WMD material	
Transmission of WMD-relevant knowledge	
Fabrication of false end-use certification	
Enlisting of transportation services	✓
Enlisting of financial services	✓
Use of crypto-currencies	
Recruitment of combatants	✓
Recruitment of children into war	✓
Commercialization of conflict minerals	✓
Commercialization of wildlife and wildlife products	✓
Conducting and promoting hate speech or hate crimes	

The lack of resolve among policy-makers to address all vulnerabilities created by malicious uses of digital technologies has allowed the private sector to accept major flaws in their commercial compliance mechanisms. In essence, current tools flag designating individuals and entities, as well as their social networks. But they do not help to prevent a long list of other violations.

Sanctions measures	Existing Commercial Compliance Tools
Targeted measures - Assets Freeze	✓
Targeted measures - Travel Ban	✓
Sanctions against the provisioning of financial services	✓
Sanctions against the provisioning of fuel	✓
Embargo against raw materials	unresolved
Due diligence requirements for trade of conflict minerals	unresolved
Embargo against conventional arms	unresolved
Embargo against conventional dual use items	unresolved
Embargo against nuclear components, technologies, knowledge	unresolved
Embargo against dual use nuclear material	unresolved
Embargo against chemical and biological components	unresolved
Embargo against ballistic missiles materials and technologies	unresolved
Items that fall under the Catch-All provision	unresolved

Long-term efforts

While efforts are underway to meet these known challenges, we need to focus on the "unknown unknowns" that result from rapidly evolving digital technologies that already surpass conventional governance concepts. Some parts of a new, one might call it "beyond Google" cyberspace, are no longer easily constricted within national boundaries or sovereign controls. That is, unless a state or an international organization such as the UN can figure out how to stop someone from utilizing these most advanced types of technologies - for example in a scenario where 32-bit encryption is used in distributed cloud computing or perhaps using private blockchain technologies.

Threats built on such technologies easily tend to exceed national capacities for observation or interception, as the most famous example of the virtual marketplace Silk Road has demonstrated. Drugs, arms and many other illicit of illegal activities occurred on that blockchain network while remaining invisible to users of the conventional Internet, and even authorities in the technologically most advanced countries did not spot Silk Road had it not been for a coincidental discovery outside of the digital space.

What to do?

Based on the recognition that digital technology represents both a threat and an opportunity, we propose, as future steps envisaged beyond today's discussion, that a collaborative exploration, contingent on sustained Member State support, be undertaken in the form of an interactive exercise between two working groups -- one international regulatory and the other technical -- comprised of experts from states and the private sector. We are looking forward towards developing the specific agendas for such working groups.

***