ISPI
ITALIAN INSTITUTE FOR INTERNATIONAL POLITICAL STUDIES

COMMENTARY
3 May 2018

# GIVE DIPLOMACY A CHANCE:OSCE'S RED LINES IN CYBERSPACE

Luigi Martino

Scuola Superiore di Sant'Anna

The oday, it is an incontrovertible fact that the battle-field has become virtual, just like the ability of cyber weapons to bring about real damage [1]. The very actors in the field, even though their roles are well defined, are not the classic protagonists of international relations. The clearly defined cyber arena encompasses a number of stakeholders that are no longer just states, but also non-state actors, multinational companies, terrorists, individuals. All these stakeholders are confronting each other in the cyber arena without a regulatory framework.

The low barrier of access to Information Communications Technologies (ICT) capabilities, the speed of technological advances and the complexity of the cyber environment with regard, for instance, to traditional legal definitions of national borders, have presented new challenges to states, such as the inherent complexity of accurately attributing cyber-attacks or to well define red lines in deterrence terms.

It is both this complexity and the frequent insistence of states (and non-states) actors to attribute cyber-attacks "beyond a reasonable doubt" that gives one the ability to deny responsibility and frustrate attempts to engage a meaningful dialogue based on mutual trust and transparency in order to avoid conflict in cyberspace [2].

Moreover, alarming indicators show a) how the number of cyber incidents threatening the security and safety of states and citizens is dramatically increasing and b) the growing number of cases in which nation-state actors are involved in these malicious cyber events [3]. In other words, the current situation highlights, clearly, the ongoing difficulties to adopt effective countermeasures in order to manage cyber threats at international level, and at the same time, shows how states "have clearly tried to treat the symptoms of the malady rather than its causes" [4].

Alessandro Politi, Director of the Nato Defense College Foundation; Giuseppe Cusimano, Security and Communication Specialist

## RED LINES, HOTLINE OR LINES IN THE (CYBER) SAND? THE GOOD LESSON OF BAD EXPERIENCE

Recognizing the urgency of addressing the potential tensions arising from the (ungoverned) cyber domain, analysts and policy-makers have started to explore ways to limit malicious activities in cyberspace that could affect international peace and stability.

For instance, international actors such as the United Nations (UN), the Organization for Security and Cooperation in Europe (OSCE), the G7 and the Organization of American States (OAS), have launched specific initiatives in order to enhance stability, improve cooperation, and increase trust and transparency among states in the cyber arena. These initiatives include, in general, the identification of common norms for responsible state behaviour and, in particular, operational measures in order to reduce the risks misperception, military escalation and political tension in cyberspace [5] - In other words, the main goal of all these initiatives is to apply specific "red lines" in cyberspace and find "rules of the game" elaborating a specific reference framework in order to manage cyber incidents and cyber attacks.

The main activity (in progress) that has paved the way for the political and diplomatic actions in cyberspace was lunched by the OSCE with the specific mandate to find confidence building measures (CBM) suitable for cyberspace [6]. This initiative started on 26 April 2012, when the OSCE created a dedicated informal working group (IWG) aimed at developing CBMs to reduce the risks of conflicts in the cyber domain [7]. The IWG's work has produced relevant concrete results. In 2013, for instance, all the OSCE participating states approved an initial set of 11 CBMs focused mainly on transparency measures, communication channels, and trust among states. In March 2016 participating states endorsed a second set of CBMs [8].

The CBMs' approach has proved its very effective capabilities as a crisis prevention mechanism during the Cold War era establishing efficient red lines between the two main actors. As OSCE's "core business", the CBMs approach is able to "establish international level of expectations about states' behaviour in cyberspace" [9] with the purpose to improve stability and encourage trust, cooperation and transparency among states. In other words "such measures are designed to resolve crises and conflicts, and to support a more accurate and reciprocal assessment of matters related to mutual security" [10].

Even though these are only "voluntary" initiatives, they have favoured a minimum standard for regional cooperation in cyberspace involving top players such as Russia and the United States in the CBMs process. As far as the "red line" approach is concerned, OSCE's CBMs framework, applied to cyberspace, offers operational tools of intervention in order to enhance transparency and cooperation among states. In particular, OSCE's CBMs establishing the relevance of: information sharing; predictability of states' posture; critical infrastructures integrity; and protected communication channels.

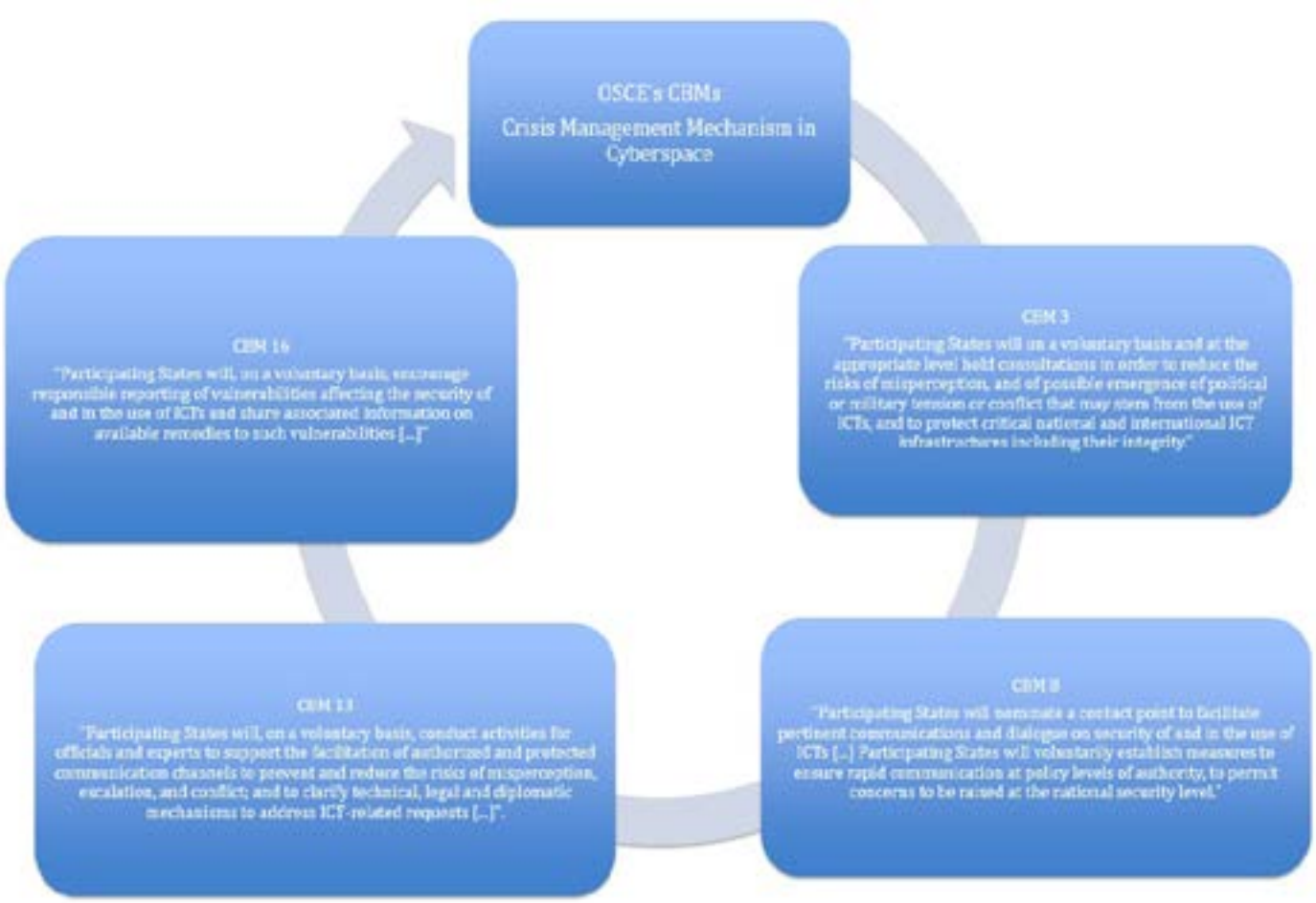
All of these initiatives might be grouped into two main clusters: transparency and cooperation measures.

- At the transparency level, CBMs 1, 4, 7, 9, 10, 14, and 16 encourage states to share information to read and understand their posture in the cyber arena in order to improve predictability of state behaviour in cyberspace.
- Regarding the cooperation measures, CBMs 2, 3, 5, 6, 8, 11, 12,13 and 15 have the main purpose to increase dialogue initiatives through information sharing and communication channels in order to avoid risk of mili-

tary and political escalation in cyberspace stemming form the malicious use of ICTs.

For what concerns the transparency level, in line with the OSCE purposes, the CBMs have allowed participating states to improve their predictability and confidence in the cyber arena. In particular, thanks to "targeted" CBMs, specifically provided to prevent military and political escalation in the OSCE region (i.e. CBMs n. 1, 4, 7, 9 10, 14 and 16), the OSCE has created a specific "transparency framework" based on two main aims: 1) to create (and use) a protected and secure communication channel and, 2) to establish transparent and clear indications on how states perceive and interpret threats and risks stemming from the cyber arena. This framework allows, ultimately, participating states to avoid the risk of misperception and mistrust in cyberspace.

The cooperation measures mean, in practical terms, that in case of cyber incident or cyber attacks, OSCE's participating states should apply a specific crisis management mechanism, in particular involving CBMs 3, 8, 13 and 16, as shown by the following figure:



According to the abovementioned OSCE's CBMs framework, in case of cyber attacks and cyber incidents, participating states (on voluntary basis) should apply a specific crisis management mechanism in order to avoid warfare and conflict stemming from the malicious use of ICTs. But this mechanism (during its first operational test) has shown a specific weakness. Indeed, in occasion of the massive cyber attacks suffered by the Ukrainian power grid infrastructures, the CBMs' crisis management mechanism was not applied.

Why? There is a non-simple and unique answer. From a political perspective, this specific case has highlighted that: a) at the moment it is difficult - in technical terms - to bypass the attribution problem (in practice: there is not an incontrovertible evidence on Russian's responsibility) and at the same time it is difficult to establish a winning deterrence (i.e. red lines); and b) CBMs are based on voluntary "commitments" and more probably Ukraine has preferred to shifting the crisis management from a cooperative approach (i.e. OSCE) to a bilateral defensive framework (including US in primis).

In practical terms, the non-application of the OSCE mechanism has shown the specific weakness of the CBMs based on a voluntary commitments framework. This limitation is emphasized not only by anonymity and uncertainty, but also due to the vagueness of CBMs itself. In other words, the Ukrainian "cyber affair" has demonstrated how CBMs, in order to well establish "real" red lines, need an "operationalizing process" based on a specific step-by-step practices implemented within the framework of relevant policies and international commitments [11].

## CONCLUSIONS: GIVE DIPLOMACY A CHANCE

Although we are witnessing the consolidation of the (cyber) battlefield, (cyber) weapons, and (multi) actors, the cyber arena is chaotic and therefore dangerous due to the lack of "rules of the game", an essential element for governing violence and preventing military and political escalation.

The militarization of cyberspace, officially decreed by the NATO Summit in Warsaw in 2016 [12] (but de facto sanctioned over the last decade by various military doctrines and national cyber security strategies), has removed any doubt about the intention of states to consider cyberspace as a sphere of military conflicts, even if this area was originally created with purely technological features [13].

The OSCE became the first regional organization to approve comprehensive and specific sets of measures with the aim to reduce the risk that a misunderstanding related to cyber initiatives could create instability and political escalation. Although this process is legitimated by the unanimous consensus of participating states, in practice CBMs required a specific "action plan" given that "where politically binding CBMs are consistently, uniformly implemented over a significant period of time, they may gradually lead to the formation of new rules in customary international law" [14].

More importantly, the OSCE's CBMs represent an attempt to set into motion a fruitful approach, with the lofty goal of initiating an appropriate political process in order to define a clear and shared legal framework and create boundaries, or red lines, on what is the acceptable states' behaviour in the digital sphere.

1. Joseph Nye, Deterrence and Dissuasion in Cyberspace, International Security 2017 41:3, 44-71.

2. As Nigel Inkster has observed: "The evolution of the cyber domain […] has significantly complicated this picture, not merely in terms of how armed forces adopt and adapt to new technology, but in terms of raising questions about what constitutes military use in a domain where civilian and military users

are inextricably entangled, and in which many cyber capabilities that are not obviously military in purpose can be used to generate militarily relevant effect." See Nigel Inkster, Measuring Military Cyber Power, "Survival", vol.59, no. 4 August-September 2017, pp. 27-34.

3. In this case it is relevant the "Cyber Operations Tracker" edited by Council for Council on Foreign Relations which contains almost 200 state-sponsored attacks by 18 countries since 2005, including 20 in 2016;

4. Jason Healey and Tim Maurer "What it'll take to forge peace in cyberspace" published by "Christian Science Monitor", March 2017.

5. Paul Mayer, Diplomatic Alternatives to Cyber-Warfare, "The RUSI Journal", 157:1, pp. 14-19; and Anna-Maria Osula and Henry Rõigas (Eds.) International Cyber Norms: Legal Policy and Industry Perspectives 2016, Tallinn, NATO CCD COE Publications.

6. For more information see https://www.osce.org/secretariat/cyber-ict-security.

7. OSCE Permanent Council Decision no. 1039.

8. OSCE Permanent Council Decision no. 1106 and Permanent Council Decision no. 1202.

9. Patryk Pawlak, Confidence-Building Measures in Cyberspace: Current Debates and Trends, pp. 129-153 on Anna-Maria Osula and Henry Rõigas (Eds.) International Cyber Norms: Legal Policy and Industry Perspectives, NATO CCD COE Publications, Tallinn, 2016.

10. International Institute for Strategic Studies, "Evolution Of The Cyber Domain: The Implications For National And Global Security", IISS Strategic Dossier, 2015.

11. International Institute for Strategic Studies, "Evolution Of The Cyber Domain: The Implications For National And Global Security", IISS Strategic Dossier, 2015.

12. NATO Summit Warsaw 2016, [online] http://www.nato.int/cps/en/natohq/events_132023.htm; regarding the specific statement on cyberspace see CCDCOE NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit, [online] https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html.

13. Kenneth Geers, World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks "Fire-Eye Labs", 2014, [online] http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf; moreover, see Michael N. Schmitt and Liis Vihul, Proxy wars in cyberspace: The Evolving International Law of Attribution, "Fletcher Security review" | vol I, issue II Spring 2014.

14. UN General Assembly, 'Annex II: Draft Guidelines for Appropriate Types of Confidence –Building Measures and for the Implementation of Such Measures on a global or Regional Level', in Report of the Disarmament Commission, A/41/42, 23 June 1986.