




Sanctions Against Cyber-

Attacks:

**Effective Coercion or
Idle Threats?**

EKATERINA MARTYNOVA
**'International Law in the Digital Age' Research
and Study Group**
June 30, 2020

Contents

- 
- 01 Theoretical Framework**
 - Terminology
 - US and EU regimes
 - Threefold role of sanctions as a reaction to cyber-attacks
 - Attribution
 - 02 Practical cases**
 - Cyber-attacks resulting in sanctions
 - Case study: NotPetya
 - How to measure sanctions effectiveness?
 - 03 Tentative hypothesis and preliminary conclusions**



Theoretical framework

Terminology



U.S. Executive Orders

Executive Order 13694 of April 1, 2015 as amended by Executive Order 13757 of December 28, 2016

“**steps to address national emergency**” caused by significant malicious cyber-enabled activities and “**prohibitions**” aimed to deal with this threat

EU Regulation

Council Regulation (EU) 2019/796

“**restrictive measures**” against cyber-attacks threatening the Union and its Member States

“Steps”, “prohibitions” and “restrictive measures” by their nature constitute **sanctions** and their imposition is commonly described as imposition of a “sanctions regime”.

I will address “sanctions” as the main countermeasure to cyber-enabled activities by which I mean unilateral or collective coercive measures taken against a person, an entity or a State to force it to behave in a particular way (e.g. stop cyber operations), or as a punishment for not doing so, or a deterrence measure (both for the aggressor and the third parties).

US and EU Regimes



	US	EU
Legal basis	Executive Orders of the US President 2015, 2016 Countering America's Adversaries Through Sanctions Act (CAATSA) 2017	EU Council Regulation 2019
Measures	<ul style="list-style-type: none">• blocking the property located in the United States• denial of access to the U.S. financial market• prohibition to provide funds, goods or services to the sanctioned persons• travel ban	<ul style="list-style-type: none">• prevention of the entry of the sanctioned into, or transit through, territories of EU Member State• funds and economic resources freeze
Procedure of imposition	At the discretion of the U.S. President	Listing and delisting the aggressors is within the exclusive competence of the Council. The Council's decision shall be taken unanimously upon a proposal from a Member State or the High Representative of the Union for Foreign Affairs and Security Policy.

Threefold role of sanctions as a reaction to cyber-attacks



a **countermeasure** to the malicious actions in the cyber space

01

02

a measure of **responsibility**, punitive measure on the non-State actors and States – sponsors or facilitators of cyber operations



a measure of the twofold **deterrence**:
(i) of the aggressive State from engaging in additional belligerent behavior; (ii) of other countries not to engage in similar activities

03



Attribution



Technical aspects

- Monitoring and logging
- Computer forensics
- Passive tracking ('honeypots', 'beacons', etc.)
- Active tracking ('hack-back', 'false flags')



Intelligence aspects

Human and signal intelligence



Geopolitics of attribution

- *Cui bono?*
- Was it a "false flag" operation?

- In States' practice credible attribution of cyber-attacks is not an indispensable prerequisite for sanctions imposition.
- Are economic sanctions indeed a measure to protect States' national security in cyber space, or just another bullet in the trade wars?



Practical cases

Cyber-attacks resulting in sanctions



Meddling into the US Presidential Elections

2014

- Attributed to Russia
- 2017: U.S. sanctioned 9 Russian entities and individuals
- 2018: further sanctions on 5 entities and 19 individuals
- 2019: sanctions against 7 Russians as a warning against foreign interference in US 2020 elections

May 2017

NotPetya

- Attributed to Russia
- March 2018: U.S. sanctions against 3 entities and 13 individuals under E.O. 13694; and 2 entities (FSB and GRU) and 6 individuals under section 224 of CAATSA
- June 2018: 5 entities and 3 individuals sanctioned under E.O. 13694 and CAATSA

The Sony Pictures Hacking

- Attributed to North Korea
- U.S. sanctioned 10 individuals and 3 entities associated with the North Korean government

2016

WannaCry

- Attributed to North Korea
- 2019: three North Korean hacking groups were sanctioned under E.O. 13722 as agencies, instrumentalities, or controlled entities of the Government of North Korea

June 2017

Case study: NotPetya



Attack

- > 27 June 2017: a major global cyber attack began, Ukraine
- > Infections in France, Denmark, Germany, Italy, Poland, the UK, the US, etc.
- > 80% of all infections were in Ukraine, with Germany second – 9%



Damage

- > financial costs amounting to 0.5% of Ukraine's GDP
- > \$1.2 bln losses for companies globally
- > crucial infrastructure lockdown



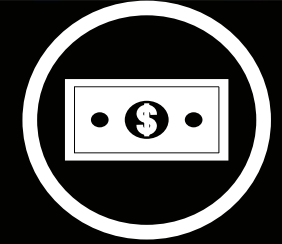
Attribution

- > February 2018: Australia, Canada, Denmark, Japan, New Zealand, the UK and the US formally attributed NotPetya to Russia



US sanctions round 1 March 2018

- > 3 entities and 13 individuals under E.O. 13694
- > 2 entities (FSB and GRU) and 6 individuals under section 224 of CAATSA



US sanctions round 2 June 2018

- > 5 entities and 3 individuals under E.O. 13694 and CAATSA

How to measure sanctions effectiveness?

Cost-benefit analysis

A systematic approach to estimating the strengths and weaknesses of alternatives used to determine options which provide the best approach to achieving benefits while preserving savings. The analyst sums the benefits of sanctions and then subtracts the costs associated with their implementation.

Game theory

Modelling of strategic interaction among States as rational decision-makers. Is the interaction 'cyber-attack – sanction' a zero-sum game?

Theory of Mansur Olsen

Analysis of sanctions impact on behavior and rhetoric of the aggressive State's political elites - well-organized group with properly defined stimuli system punishing those deviating from group profit-maximizing behavior.



Tentative hypothesis
and preliminary
conclusions

Hypothesis (1 of 2)



My tentative hypothesis is that the watershed between sanctions as effective coercive measures and idle threats lies in the multi-criteria decision analysis by policymakers.



Correlation of the sanctions with the structure of economy of the targeted State

For the Russian economy, such factors as slumping prices on the traditional export products have a much more significant impact than certain sanctions introduced. High oil prices, on the contrast, enable Russia to restore its financial reserves and mitigate the worst impact of economic sanctions



Short-term effects vs medium- and long-term damage to the country economy and sanctioned actors

In the cyber space actors may not have long-term aspirations – no pressure points which sanctions can effectively target



Credibility of sanctions and consistency of their application

Cyber-attacks are literally happening hundreds of thousands of times a day. However, only a small fraction of cyber-attacks trigger imposition of sanctions. Criteria to sanction particular countries, individuals or companies should be clear, and practice of their implementation – consistent

Hypothesis (2 of 2)



Costs of designing and implementation of sanctions

Designing, discussing, evaluating, implementing, monitoring, reflecting and correcting sanctions entails direct and indirect costs. The existence of these costs and their significant amount in our real (non-Coase) world determines the fact that only significant cyber-threats are punished



Standards of substantiation

The U.S. regulation requires “significant threat” to national security, “significant disruption” to the availability of the computer network, “significant misappropriation” of funds or economic resources as a precondition for imposition of sanctions on the alleged offender. Similarly, the EU regulation targets cyber-attacks with a “significant” effect that constitute an external threat to the EU and its Member States. The standards of evaluation of the “significance” of threats and effects of cyberattacks shall be established and observed



Application of sanctions in conjunction with other tools of diplomacy

A stack of several coins, including a gold coin, is placed on top of an old newspaper. The newspaper has some text visible, including the word "Gottlieb". The background is dark and textured.

Preliminary conclusions

Analysis does not provide conclusive findings that economic sanctions *per se* are an effective counter-measures against cyber-attacks.

From the analytical point of view, when various measures are put in place, it is hard to assess the extent to which the economic sanctions contribute to the eventual outcomes.

Economic sanctions generally inflict economic costs to all countries involved in the sanction episodes, including those taking the sanctions, thus shooting themselves in the foot.

The effectiveness of sanctions is further reduced today due to a growing interdependency between markets and a 'shrinking world'. It is the combination of various interventions that could eventually make the sanction effective coercion against cyber-attacks and not idle threats, but not the economic sanctions *per se*.



Thank you