

1

Diplomatic Measures in Response to Russian Cyber Operations

Following Russia's cyber operations directed against political parties in 2016 (the Macron campaign and the U.S. Democratic Party), alongside international organizations (OPCW), Western governments responded with a series of countermeasures.

COUNTERMEASURES



Public attribution and naming & shaming:

The highly detailed Dutch attribution following the OPCW hack, in tandem with the previously released details from the Skripal attribution by the U.K., eventually led to a major data breach disclosing the identities of over 300 GRU officers



Indictments: The U.S. indicted 12 GRU officers for the 2016 presidential election hacking and the OPCW hack. European partners did not join this effort.



Sanctions: Whilst the U.S. was quick to enact sanctions against Russia for its actions, the EU and its member states remained reticent to employ similar actions, despite its Cyber Diplomacy Toolbox.



Diplomatic Expulsions: The U.S. expelled 35 Russian diplomats for the 2016 election interference; a coordinated European response had 19 member states expelling Russian officials.

SECOND-ORDER NORMATIVE EFFECTS

Highly detailed attribution may set a precedent for and inherently contribute to the Russian narrative that a burden of proof is required by the victim.

Politicizing indictments can escalate lawfare. As a result, states like Russia and China may act more aggressively and freely to politicize international law enforcement as a response.

The second order-normative effects of sanctions were not considered in this case.

The second order-normative effects of diplomatic expulsions were not considered in this case.

NORM EMERGENCE

Norm prohibiting cyberoperations against electoral infrastructure

The entrepreneurs, initially the GCSC and later the French government (using the Paris Call as organizational platform) and Dutch government (using the UN as organizational platform), framed the norm to threats to democracy and sovereignty, and linked it to the existing norms on non-intervention and critical infrastructure protection.

