2

Responding to Russian Disinformation in Peacetime

Between 2016 and 2018, Russia conducted disinformation campaigns targeting the U.S. presidential and mid-term elections, and the French presidential election.

Countermeasures

Resilience: The Macron campaign used tested information security measures to pre-empt, delay, discredit and minimize the effects of Russian disinformation

Discredit Media as Propaganda: The Macron campaign disaccredited Russian media outlets Russia Today and Sputnik as propaganda and threatened legal action.

Offensive Cyber Operations: The U.S. embarked on an offensive cyber operation against the Russian troll factory "the Internet Research Agency", effectively shutting it down for several days.

Cyber Pre-Deployment: The U.S. pre-deployed malware within Russia's critical infrastructure. This amounted to a means of coercive signaling to deter further Russian interference.

Second-order normative effects

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

This may set the precedent for other political actors to employ similar measures against legitimate journalists on the same basis.

In responding with offensive cyber effects, the U.S. implied that it is now acceptable to hack what one considers 'fake news', and that it perceives and weaponizes information in the same way as Russia.

While U.S. actions did not violate the UN norm prohibiting cyber operations against critical infrastructure, these actions still implied that the U.S. has implicitly accepted a norm of mutual hostage taking in cyberspace.

Norm proposal

A norm against disinformation as covert election interference

If entrepreneurs would pursue such a norm proposal, it can be *framed* to covert election interference and *linked* to the non-intervention principle. Doing so would prohibit covert influence operations aimed at undermining democratic processes, while still allowing the West to overtly promote democratic principles abroad.