International Conflicts in Cyberspace

Alex Gamero-Garrido, Massachusetts Institute of Technology
SM Candidate, Engineering Systems Division
Start: May 2013 - Technology and Policy Program
Research Group: Explorations in Cyber International Relations, MIT-Harvard.
Advisor: Prof. Nazli Choucri, MIT Political Science. Co-Advisor: Dr. David Clark, MIT CSAIL.

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

Cyber Security & The Governance Cap:
Complexity, Contention, Cooperation. MIT, January 6 and 7, 2014

GLOBAL FINDINGS

Actors: international & public-private cooperation essential. New players: activists & shady State contractors. U.S., Russia & China most significant actors.

Socio-Political: Most cases related to "physical" conflicts. Awareness has increased. Diverse goals & targets.

Tools: DDoS most common. Attackers not always savvy. Air-gapping insufficient.

Sophistication: State-backed and for-profit increasing the most.

Outcome: Economic hard to estimate, incentives not to report. >2/3rd cases within a handful of jurisdictions, not global.

Accountability: hard to assign, which is valuable for States. Lower entrance barriers, cost & consequences.

THE STUDY

Method: Identify relevant cases of international nature, and their socio-political context. Extract actors, their power relationships, actions, tools, outcome. Draw inferences for individual cases as well as overall findings.

# of Cases: 17. Of which 6 global.

# of Sources: 114, both academic & media. Most cited: *A Fierce Domain* of the Atlantic Council (Healy, 2013).

SELECTED CASES

Operation Solar Sunrise

Actors: Teenagers from California and Israel; The U.S. and Israel.
Tools: Known vulnerabilities in O.S. Attacking from hosts in other countries.
Outcome: Creation of JTF-CND (US) & coordination with NIPC & Private Sector.
Insights: 80's and 90's - many attacks by teenagers with grandiose goals

Chinese Espionage

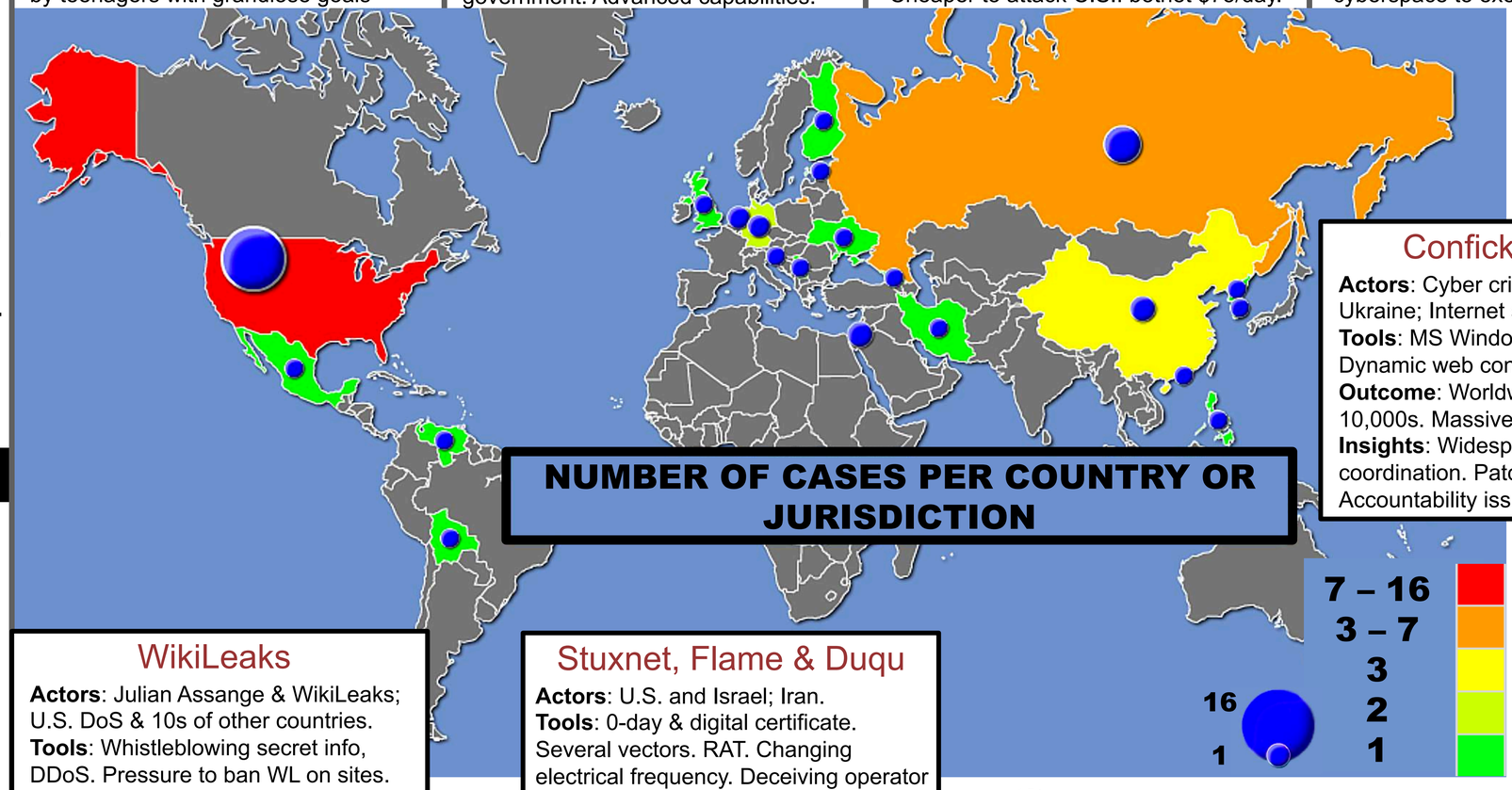
Actors: China; The U.S., allies, and over a hundred countries as targets.
Tools: 0-day, known vulnerabilities in O.S. and 3rd-party, phishing, others.
Outcome: Loss in I.P. > $250 bn. Access to advanced weapons. Use of American SW for Chinese Green Dam.
Insights: Involvement of Chinese government. Advanced capabilities.

Attacks on Estonia

Actors: Estonia, NATO & Private sector; Russia & Russian diaspora.
Tools: Spam & DDoS by botnet. ICMP, SYN & generic traffic flood. Blocking IP.
Outcome: EE cybersecurity hub. EE-Russia grew farther apart. Int'l coop.
Insights: C.S. domain for covert attacks. Developed world at higher risk. Cheaper to attack C.S.: botnet $75/day.

Russo-Georgian War

Actors: Russia & Russian organized crime; Georgia, Estonia & NATO allies.
Tools: DDoS - SQL injection & Cross-Site Scripting. Spam. 3rd country host.
Outcome: Disruption of civilian infrastructure. Russian superiority.
Insights: Some States can disrupt civilian infrastructure. Kremlin using cyberspace to exert int'l influence.



Conficker Worm

Actors: Cyber criminals, possibly from Ukraine; Internet security community.
Tools: MS Windows buffer overflow. Dynamic web control & updates.
Outcome: Worldwide victims in 10,000s. Massive for-profit botnet.
Insights: Widespread security coordination. Patches only work if used. Accountability issue: unaware victims.

WikiLeaks

Actors: Julian Assange & WikiLeaks; U.S. DoS & 10s of other countries.
Tools: Whistleblowing secret info, DDoS. Pressure to ban WL on sites.
Outcome: Massive release. U.S. spying on allies. Over 1k backups.
Insights: Reduced costs for WB. Assange's goals obscure. Undermined trust in democratic institutions.

Stuxnet, Flame & Duqu

Actors: U.S. and Israel; Iran.
Tools: 0-day & digital certificate. Several vectors. RAT. Changing electrical frequency. Deceiving operator
Outcome: Damage to 1k centrifuges in Natanz. Over 100k hosts infected.
Insights: Use of tools from cyber criminals. Equivalent to military strike. Iran now getting more involved in cyber.

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research. Map: TargetMap.