1st CYBER SECURITY WORKSHOP
"CYBER CAPABILITIES AND THEIR FUTURE USE: CHALLENGES AND STRATEGIC OUTLOOK "
KONRAD-ADENAUER- STIFTUNG TURKEY (KAS) in cooperation with THE CENTRE FOR ECONOMICS AND FOREIGN POLICY STUDIES (EDAM)
Ankara, 04.12-06.09.2019

PANEL-1: Regional powers turn to cyber capabilities: The Case of the Middle East

„The Stuxnet effect: Iran`s cyber-conflict conduct after 2010"

Kerstin Zettl, M.A.
University of Heidelberg
Institute of Political Science

gefördert durch
DSF Deutsche Stiftung Friedensforschung
german foundation for peace research

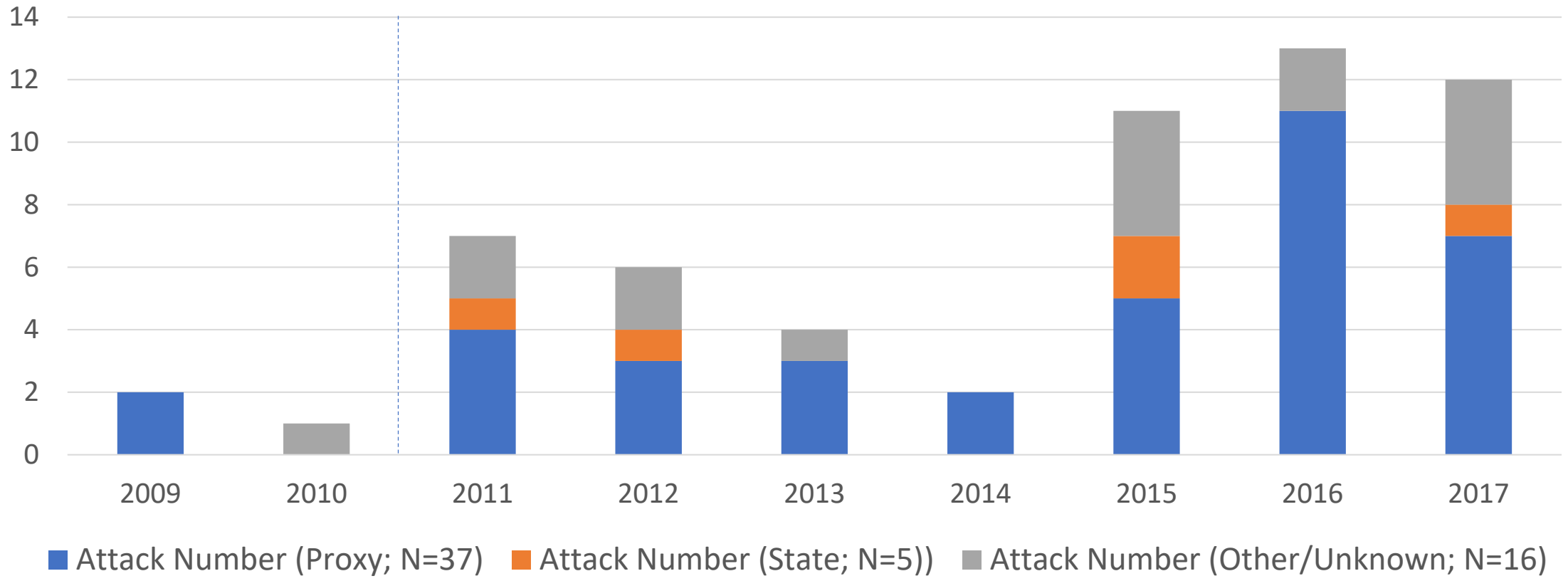
Stuxnet as the necessary cyber-„push“ to Iran?

- Stuxnet became public in 2010
- Heavily disruptive malware
- **Alleged masterminds:** USA & Israel
- **Target:** Iranian nuclear facility in Natanz
- **Effect:** Destruction of many thousand centrifuges

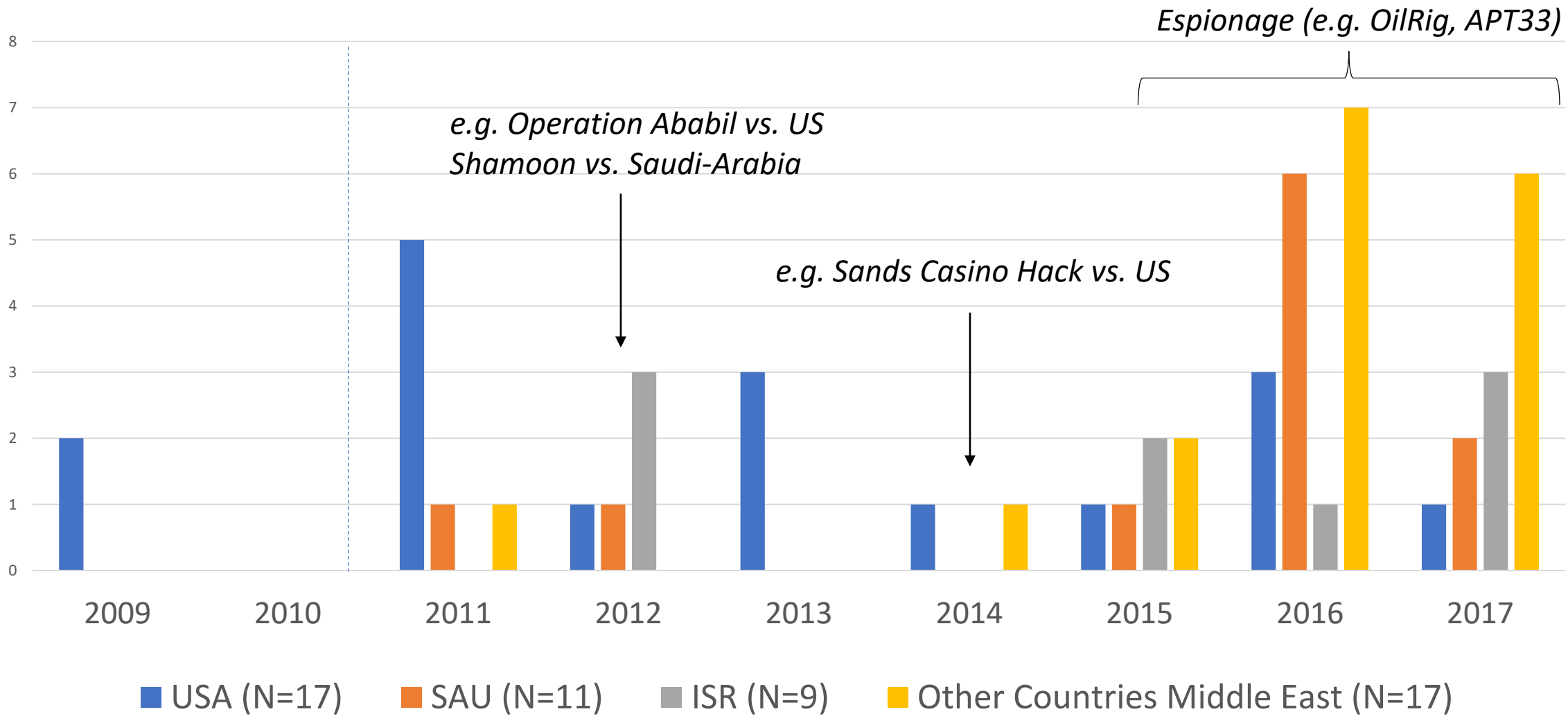
Source: Yahoo News photo illustration; photos: AP, Getty Images. Shutterstock

Question: How did Iran`s cyber-conflict-conduct evolve after Stuxnet?

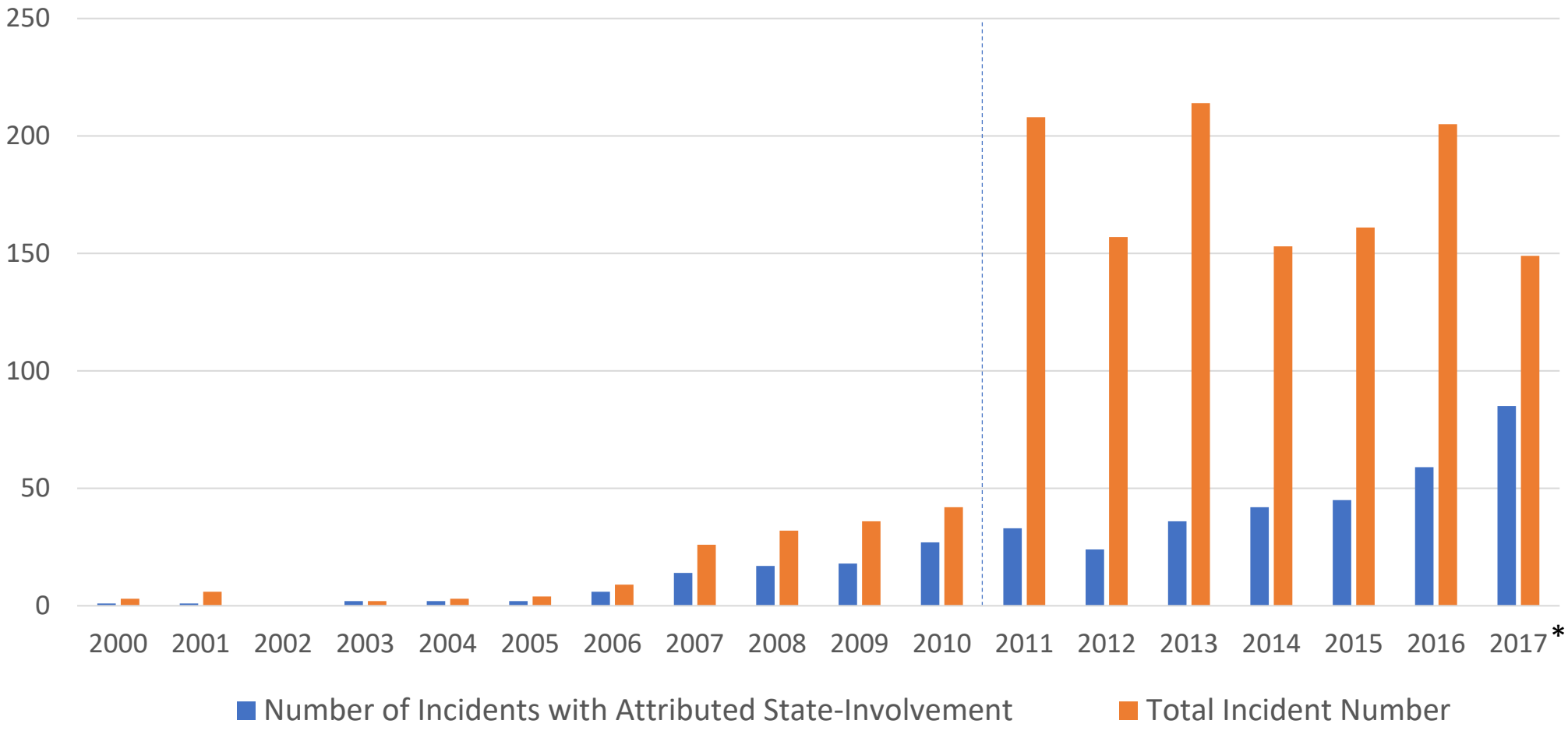
Cyber-attacks attributed to Iran from 2009 to 2017
(N=58; Source: HD-CY.CON)



Mostly affected target countries



Overall conflict-development after Stuxnet



**Preliminary Result*

Developments in Iranian Proxy-Landscape

Professionalization: From patriotic hackers mostly conducting DDoS-attacks to espionage on behalf of the state (similar to developments in the chinese hacking community a decade before)

Example: Ajax Security Team (aka Flying Kitten; before 2014 mostly defacement, afterwards malware-based-espionage; e.g. Operation Saffron Rose, targets: US-defense companies and Iranian users of anti-censorship technologies)

Source: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf

Conclusion/Questions for the future

Iran`s cyber-conflict conduct originated and heavily increased after Stuxnet in 2010, but in the long-term mostly as a complementary strategy in regional offline-conflicts.

- Iran`s reaction to US withdrawal from JCPOA (2018): Increased cyber-attacks against US-targets?
- Disruptive attacks also against western or israeli targets, due to increased offensive capabilities?
- Future integration of Iranian cyber-means in conventional conflicts?

Thank you very much for your attention!

Appendix

Obfuscating Iranian government involvement in offensive campaigns.

Source: https://www.recordedfuture.com/iran-hacker-hierarchy/

(Non-exhaustive) list of Iranian Proxies

- Cutting Kitten
- Chafer
- OilRig (aka APT34; aka Helix Kitten; aka Chrysene)
- Copy Kittens
- APT33 (aka Magic Hound)
- Charming Kitten (aka APT35, aka Newscaster)
- Domestic Kitten
- Dark Hydrus
- ...

US indictments against Iranian cyber-actors

Figure 1. Timeline of Criminal Charges Against Foreign Hackers (by filing date)

2019	May	(Unsealed May 2019)	Fujie Wang and John Doe (China) - Anthem Hack
	Feb	(Unsealed Feb 2019)	Witt et al. (Iran) - Espionage against U.S. intelligence orgs
2018	Dec	(Unsealed Dec 2018)	Zhu and Zhang (China) - MSS Cloudhopper IP Theft (APT 10)
	Nov	(Unsealed Nov 2018)	Savandi and Mansouri (Iran) - SamSam Ransomware
	Oct	(Unsealed Oct 2018)	Zhang et al. (China) - JSSD Hacking of Aerospace Cos.
	Oct	(Unsealed Oct 2018)	Morenets et al. (Russia) - GRU Anti-Doping Orgs, OPCW Hacks
	Sep	(Unsealed Oct 2018)	Elena Khusyaynova (Russia) - Project Lakhta Influence Operation
	Jul		Netyshko et al. (Russia) - DNC, DCCC Hacks and 2016 Election
	Jun	(Unsealed Sep 2018)	Park Jin Hyok (North Korea) - Sony, WannaCry, Bangladesh bank
	May		Umar Agha and Firas Dardar (2nd set of charges) - Syrian Electronic Army
	Feb	(Unsealed Mar 2018)	Mabna Institute (Iran) - IRGC-linked IP theft campaign
	Feb		Internet Research Agency (Russia) - Election influence operations
2017	Nov	(Unsealed Nov 2017)	Behzad Mesri (Iran) - Hack of HBO
	Sep	(Unsealed Nov 2017)	Wu Yingzhou et al. (China) - Boyusec IP theft
	Aug	(Unsealed Aug 2017)	Arrest of Yu Pingan (China) - OPM hack-linked malware
	Feb	(Unsealed Mar 2017)	Dokuchaev et al. (Russia) - Yahoo Hack
2016	Apr	(Unsealed Jul 2017)	Ajily and Rezakhah (Iran) - Arrow Tech IP Theft
	Jan	(Unsealed Mar 2016)	ITsec and Mersad Co. (Iran) - Financial Sector DDoS, Bowman Dam
2015	Sep	(Unsealed Mar 2016)	Peter Romar and Firas Dardar (Syria) - Syrian Electronic Army
2014	Jun		Arrest of Su Bin (China) - Boeing hack (C-17 IP Theft)
	Jun	(Unsealed Mar 2016)	Umar Agha and Firdas Dardar (Syria) - Syrian Electronic Army
	May	(Unsealed Jun 2014)	Evgeniy Bogachev (Russia) - GameOver Zeus Botnet
	May	(Unsealed May 2014)	PLA Unit 61398 (China) - Economic Espionage (aka APT 1)
2013	Nov	(Unsealed Dec 2015)	Arrest of Nima Golestaneh - Arrow Tech IP Theft

Source: https://www.lawfareblog.com/whats-point-charging-foreign-state-linked-hackers