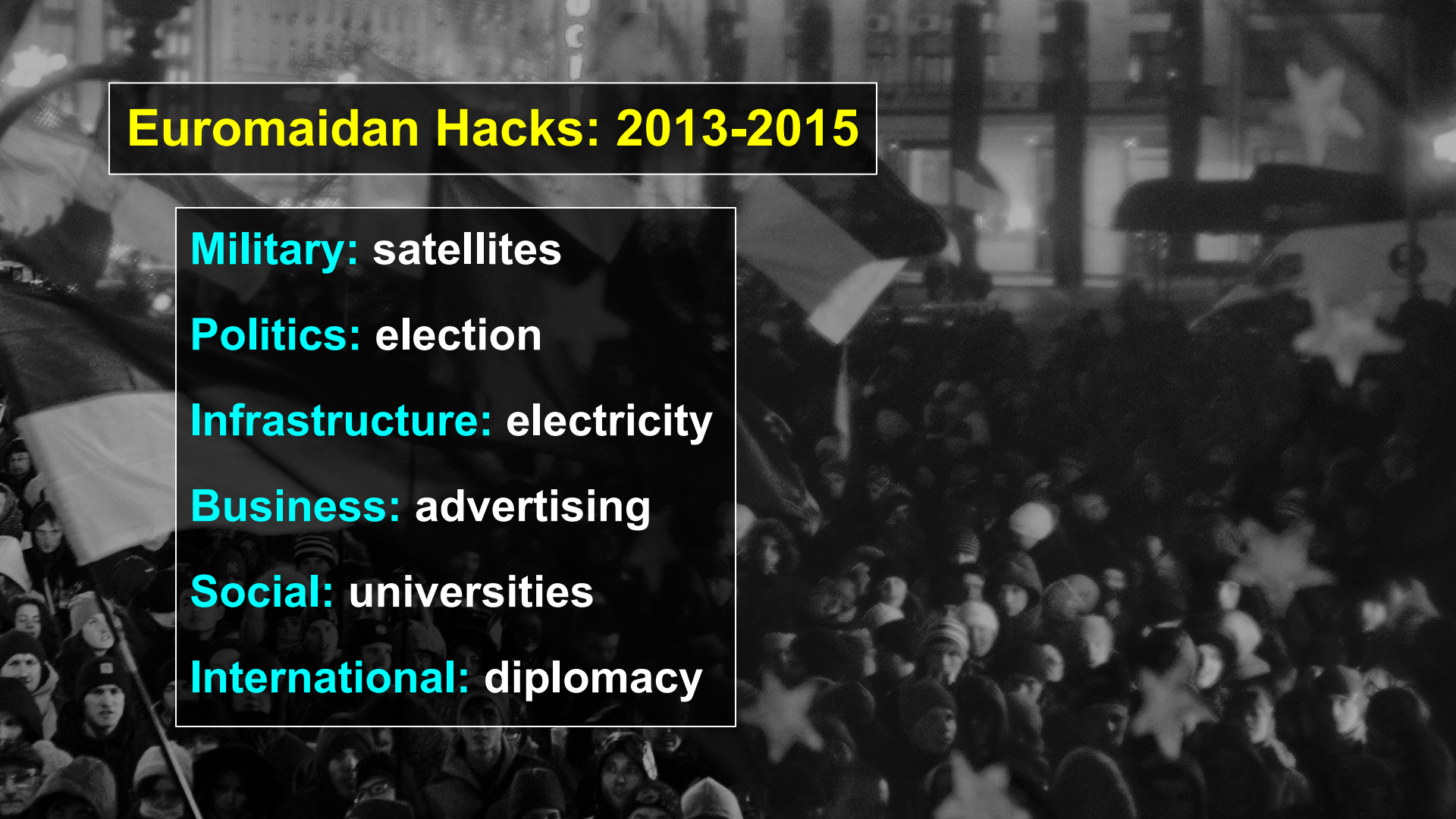

Computer Hacks
in the
Russia-Ukraine War
Kenneth Geers
Very Good Security
Aalto Univ



Euromaidan Hacks: 2013-2015

Military: satellites

Politics: election

Infrastructure: electricity

Business: advertising

Social: universities

International: diplomacy

Prepping the Battlespace

2021

6 RU APTs, 8 MW families

Jan 2022

Defacements, WhisperGate, GRU vs UA/US LNG

Feb 15-24

GRU DDoS vs UA gov

Ministerrat der Deutschen Demokratischen Republik
Ministerium für Staatssicherheit

Bezirksverwaltung Dresden

B 217590

Putin — Name
Wladimir — Vorname
07.10.1952 — Geb. am
Leningrad — Geb.-Ort
Major — Dienstgrad

Dresden, den 31.12.1985

Unterschrift


H-Hour
Feb 23
Wiper, SMS
Feb 24
Wiper, ISP, social
H -1
Viasat


?: Nuke net down before takeover
Mar 1: missile, wiper vs UA media
Mar 3: Sumy blackout, explosions
Mar 15 & 22: new wipers
Mar 19: GRU Industroyer2
Mar 28: Ukrtelecom drops 87%
Jun 27: Killnet DDoS vs Lithuania


H-Hour
Feb 24
Anonymous declares war
Feb 26
Belarusian Railways
UA SIM cards
Assassinations
Oslo
Västerås
Stockholm
Tallinn
Pskov
Tver
Moskva
Linköping
Göteborg
Aalborg
Rīga
Vitebsk
Smolensk
Orsha
Bryansk
Tula
Mogilev
Orel
Vilnius
Minsk
Gomel
Kursk
København
Kaunas
Kaliningrad
Hamburg
Białystok
Szczecin
Warszawa
Poznań
Berlin
Brest
Kharkiv
Kyiv
Łódź
Leipzig
Wrocław
Dnipro
Erfurt
Dresden
L'viv
Köln

Allies

Feb 26: IT ARMY of Ukraine

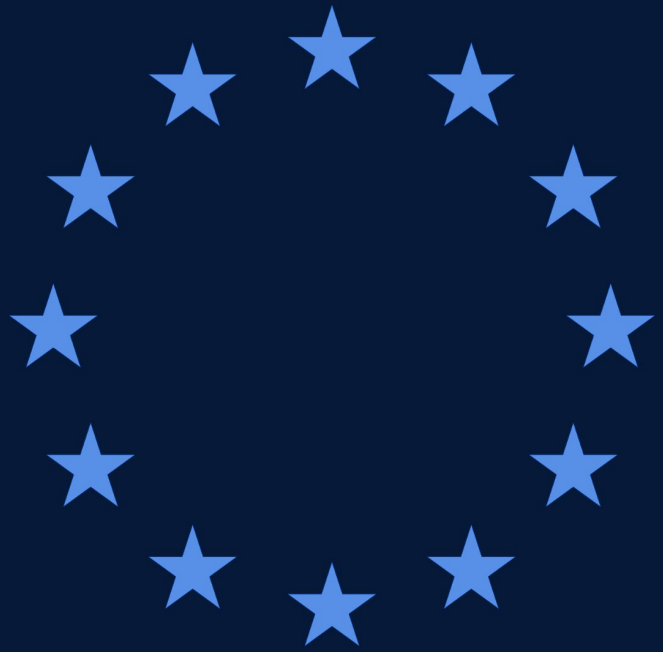
US: FBI/USAID/DOE/DHS/CISA

US Cyber Cmd: UA Cyber Cmd

WH: preemptive removal of RU MW

Dox: DDoSecrets (6M RU/BY)

RU: Belarus, China, Syria, DPRK




Connectivity
Starlink: counter-RU hack
Up: Zelensky, military
June 17: DDoS vs Putin speech
DoS RU: political question
IR: deterrence, arms control

Summary

Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep
LNG	ISP	Wiper		SORM	~~Wikipedia~~	~~Google~~		
Defacement	Firmware	ISP				Fake App		
Wiper	Power	Power			Killnet	PSYOP		
EU CRRT	BY RR	US RU op			CYBERCOM		Bots down	PSYOP
	Starlink				DDoS Putin			Geolocation
	UA SIMs							
	Anonymous							
	IT Army							
	DDoS							
	Defacement							
	Dox							
	PSYOP							
	PSYOP	Media						
	LNG							
	DDoS							
	Wiper							

Mid-War Assessment

War: decentralized, networked

CNA: disruptive, not decisive

CND: better deterrence

Cyber power: soft power

Connectivity: resilient

Attribution: quick, accurate

Cloud: back it up

Russia: bleeding hackers

Questions

Russia

Limited by CNA or CND?

Ukraine

Info Ops beat CNO?

Allies

Can diplomacy hold?

What else?


Computer Hacks
in the
Russia-Ukraine War
Kenneth Geers
Very Good Security
Aalto Univ