MAY 12-13
BRIEFINGS

The Virtual Battlefield in 2022:
Russia-Ukraine War & Its Policy Implications

Kenneth Geers
Very Good Security

Mid-War Assessment

- Before the war
  - Fear of Russian cyber
  - Fear of large-scale attack
- Evidence so far
  - Cyber integral to kinetic ops
  - Connectivity is key
  - Complexity hard to master
  - Dynamic nature favors the nimble
- Mid-war assessment
  - Info war more important
  - Alliance power for cybersecurity
- Potential escalation
  - Any cyber aces to play?

The Washington Times

TUESDAY, JUNE 16, 1992 ★★ WASHINGTON, D.C. 25 cents

Viet POWs may still be alive in Russia

Pentagon can't confirm

By Carleton R. Bryant
THE WASHINGTON TIMES

Russian President Boris Yeltsin said yesterday that U.S. prisoners from the Vietnam War were transferred by the Soviet Union and kept in labor camps, and some of them may still be alive.

"Our archives have shown that it is true, some of them, were transferred to the territory of the former U.S.S.R. and were kept in labor camps," Mr. Yeltsin said in an interview broadcast last night on NBC-TV. "We don't have complete data and can only surmise that some of them may still be alive."

Yeltsin spokesman Vyacheslav Kostikov said later that 2,800 U.S. citizens "found themselves on Soviet soil" after World War I, World War II and Vietnam, and "many were held in prison."

"Most of them have died," he said. "It's not excluded" that some may have survived.

State Department spokesman Joe Snyder said Mr. Yeltsin's disclosure, if accurate, would be a major revelation.

"I certainly have never heard any Russian or Soviet admit it," he said.

Mr. Snyder added, however, that he had no information regarding Mr. Yeltsin's comments or any new developments on the issue.

Last night, the Pentagon said it still has no knowledge that American POWs from the Vietnam era were transferred to the Soviet Union and kept in labor camps, despite Mr. Yeltsin's confirmation.

"That's the first we heard of it," a spokeswoman told Reuters news agency. "We have no knowledge or evidence. We still don't, other than the statement that Mr. Yeltsin said."

Also yesterday, Russian Gen. Dmitri Volkogonov, chief military

see POWS, page A8

Bush greets Yeltsin here 'as a friend'

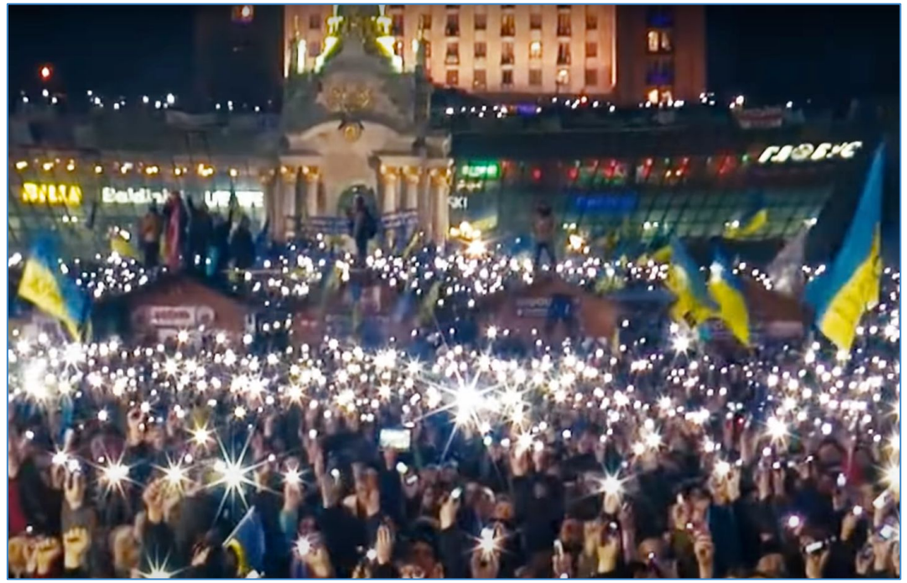
Russian bridging

is expected to leave the United States with a new nuclear dominance

Mr. Bush would not discuss spe-

1992

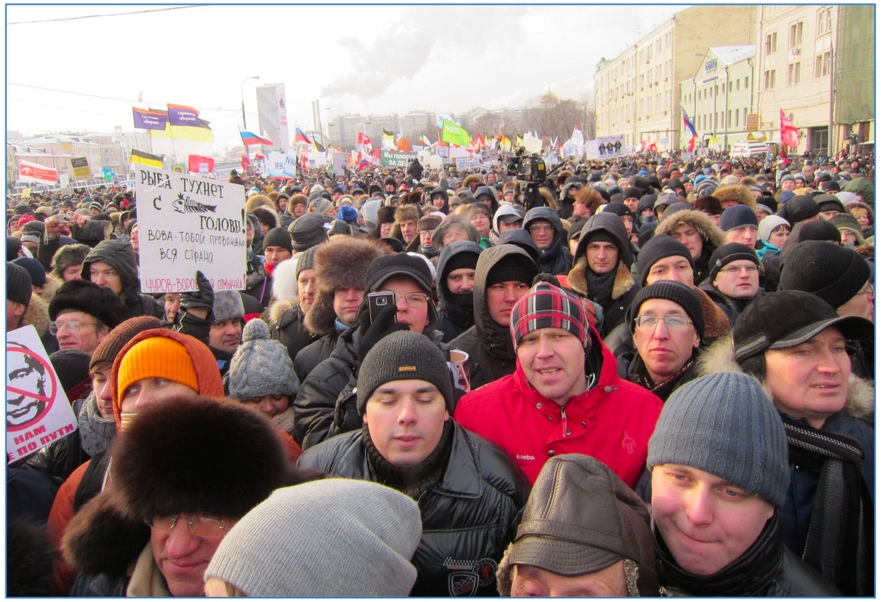
2007



2014

Что делать?

Russia
2011



Ukraine
2014

Belarus
2020

Kazakhstan
2022

Euromaidan 2014

2015 NATO book: *Cyber War in Perspective*

CERT-UA

- Cyberattacks rise w geopolitical tension
- Defacements, DDoS, espionage, false flags, doxing, physical/logical attacks on opposition servers, smartphones, sites, accounts
- Biggest attack: 2014 election

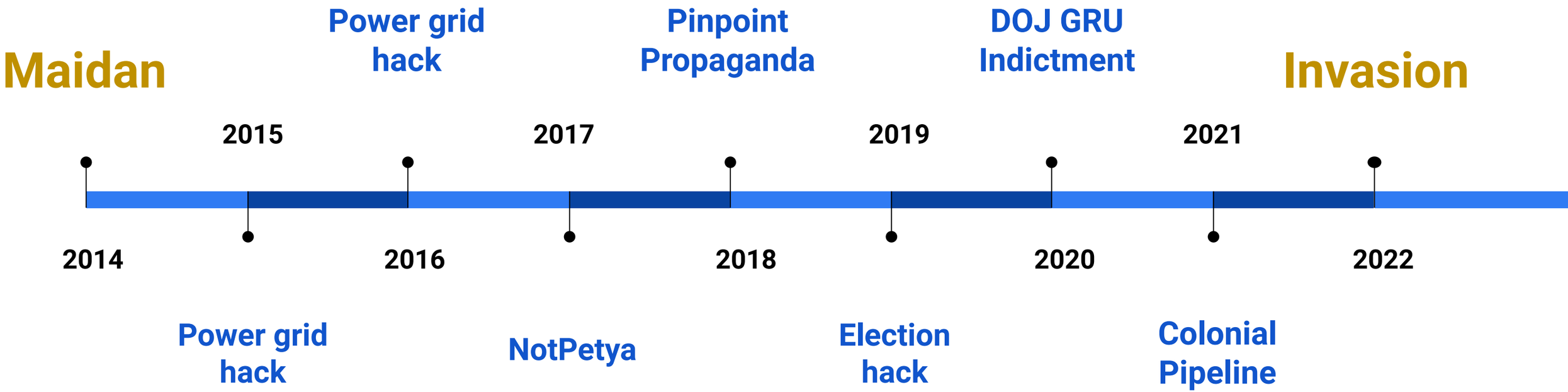
Russian military

- Severed network cables, commandeered satellites, whitewashed Wikipedia, targeted UA army via mobile phone geolocation

My students in Kyiv

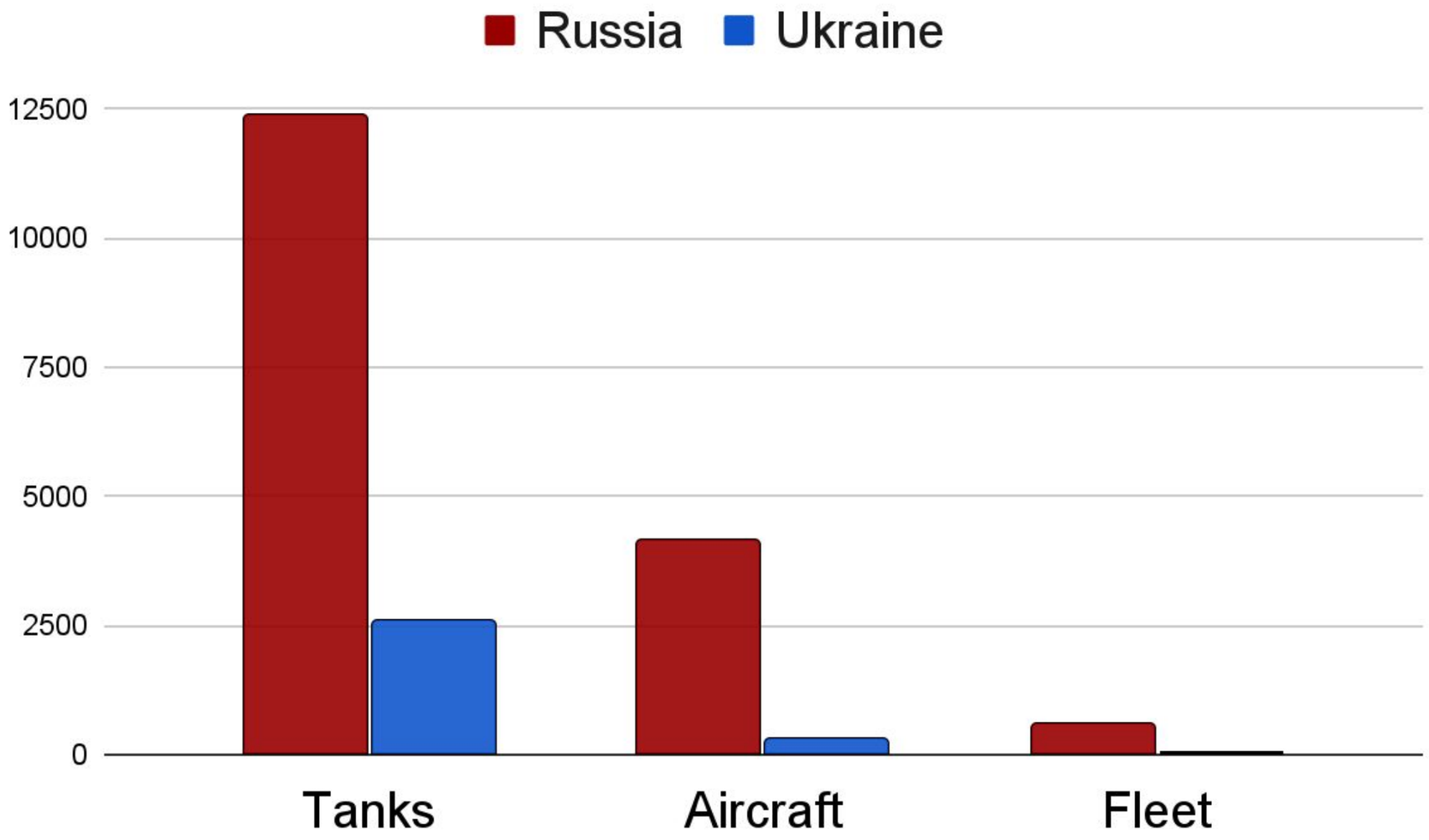
- Kremlin PSYOPS penetrated personal social media space

Peacetime in Cyberspace



Standoff Weapon

Traditional Power

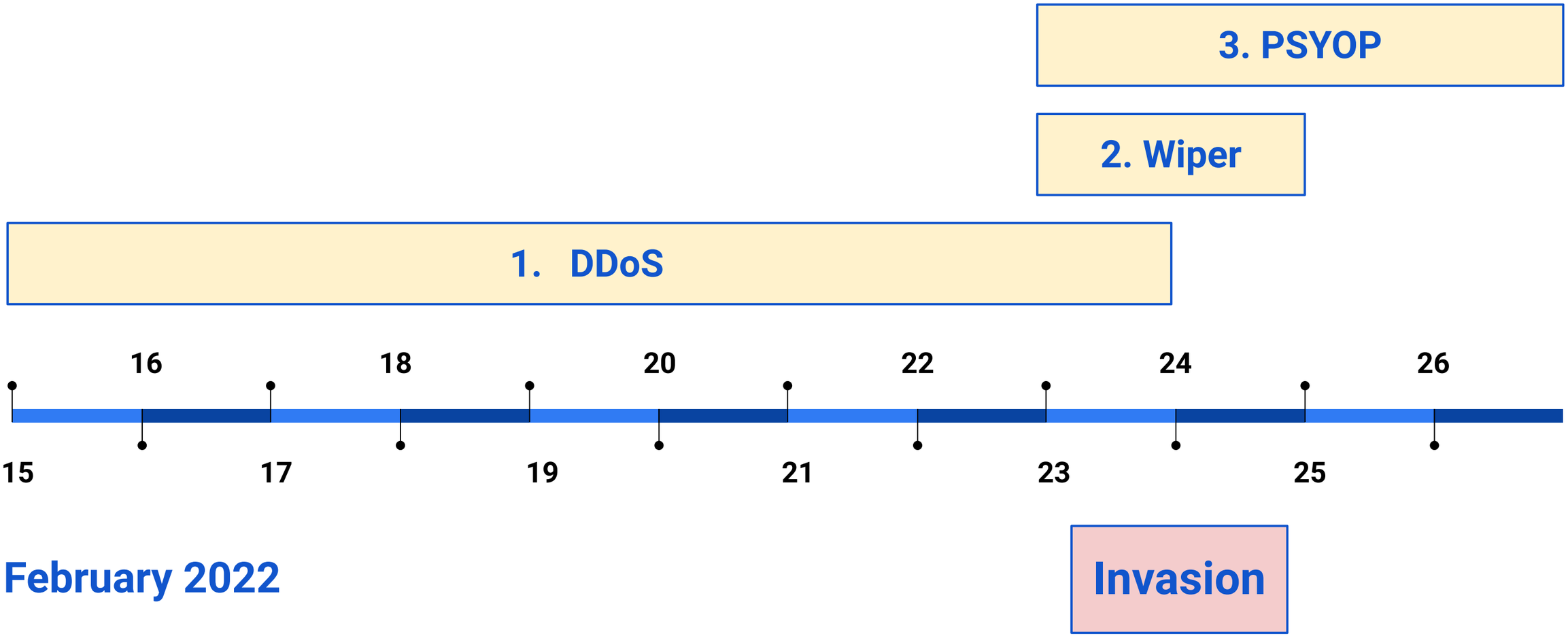


Source: Global Firepower

Cyber Power

- Info Ops
  - EW, PSYOP, CNO
- CNO
  - Collection, denial, manipulation
- Challenges
  - Attribution, asymmetry, RoE
- Autocracy
  - Info denial + fake news
- Game Theory
  - Aspirations, uncertainty

Battlespace Prep (Cyber)



1. DDoS

Feb 15-24

- Largest UA DDoS ever

Targets

- UA MoD, MFA, SBU
- Min Infra, Min Ed
- Banks, Parliament
- Cabinet of Ministers

White House

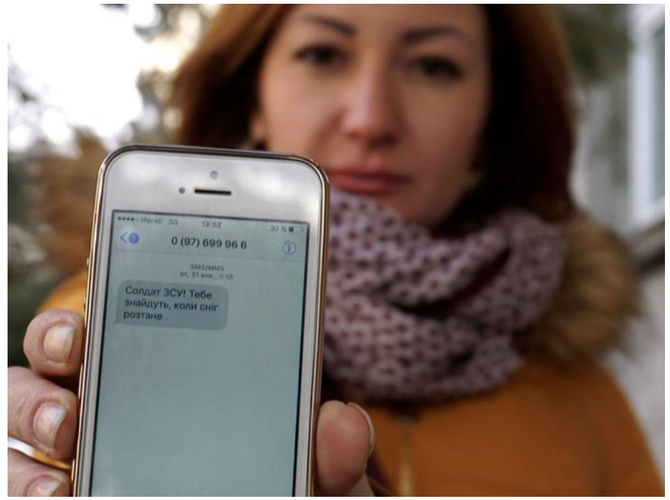
- Attribution: GRU

2. Wiper

- WhisperGate (15 Jan)
  - Encrypts files, corrupts MBR
  - Fake ransom note
- HermeticWiper (23 Feb)
  - Hours after DDoS
  - Hours before invasion
  - Signed certificate
  - Ukraine, Latvia, Lithuania
  - Artifacts from Nov 2021
- IsaacWiper (24 Feb)
  - UA gov

3. PSYOP

- Threatening SMS (23 Feb)
  - Soldiers: Flee or be killed
  - Citizens: ATMs not working
  - Government: surrender / support RU
- Hacked trusted social media / TV
  - UA mil FB: videos of soldiers waving white flags
  - FB: Ghostwriter (state-sponsored BY)
- Bots targeting US
  - Anti-vax down, pro-Russia up (24 Feb)
- DFRL: Russia testing disinformation (e.g. biolabs)
- Zelensky video (16 Mar)
  - “Lay down your weapons and surrender”
- Ukrainians familiar w RU disinfo



(AP Photo/Raphael Satter)

Air War

- RU-UA War
  - Smaller, lighter, smarter
  - Decentralized, remote-control
- Aerorozvidka
  - Crowdfunded UA SF drone unit
  - Modems, thermal cameras, 3D printers, bombs
  - Battles: 40-mile RU column, Hostomel airfield
  - Used Elon Musk's Starlink satellite system
- Bucha
  - Facial recognition: war crimes investigations
- USAF
  - More drone than human
  - Pilot, sensor, analyst
  - ROE, PTSD

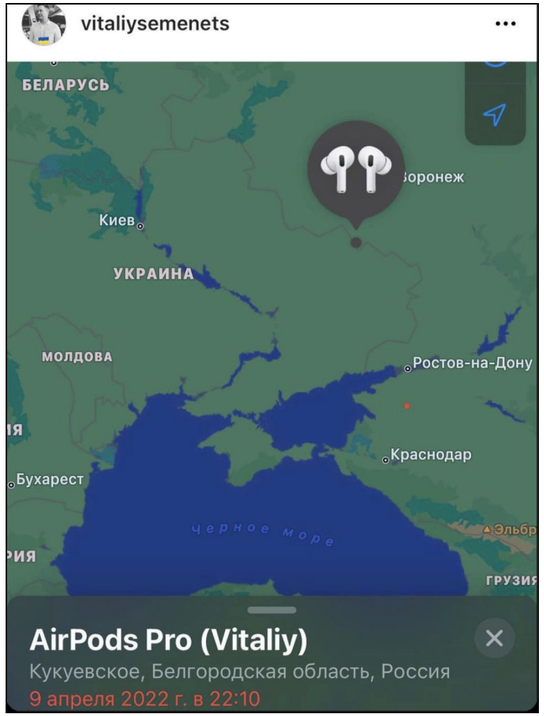
A Ukrainian soldier reviewing drone footage. Daniel Berehulak for The New York Times

Space War

- War's "biggest hack" (Feb 24)
  - Cyberattack: Viasat ground infrastructure
  - UA SSSCIP: "huge" comms loss
  - Collateral damage across Europe
- Malicious firmware update
  - Modems "unusable": must replace
- SATCOM in UA
  - Police, SSSCIP, elections
- Elon Musk
  - Starlink targeted by jamming
- Roscosmos (Mar 1)
  - Control center reportedly hacked (Net Bat 65')
  - "Stop dropping bombs, killing civilians"
- International law
  - Satcom dual use (civ / mil)

Military Comms

- Communication breakdown
  - Invasion breakdown
- Poor logistics
  - Azart radio: scandals, unpopular
- Combined arms comms
  - LCD / weakest link ∴ comms in clear
  - UA SIMs: intercept / jam / geolocate
  - RU officers targeted
- Adversary terrain
  - Adversary control (cell/wired)
- Need 3g/4g to communicate
  - Cell towers destroyed
- SBU
  - Hacker set up relay for RU mil



Hacktivism

- IT Army of Ukraine
  - UA Gov call for cyber volunteers (Feb 26)
  - Telegram channel: 300k+ subscribers
  - Form: experience, expertise, reference
  - Claim some RU hackers in ranks
- Operations
  - DDoS, propaganda, dox, defense, intel, defacements, dialogue w RU citizens
  - Targets change every day
- Challenges
  - Vetting, C&C, infiltration, mistakes, retaliation
- DDoSecrets

Anonymous

- Target RU gov websites
  - “Tango down” FSB
- Dox (Feb 25)
  - MoD personnel database
  - Leadership comms
- TV hack to show war footage
- Credit card theft
  - “Purchase weapons” for UA
- Theft from RU bank accounts
  - “Not” RU citizens, just gov (Feb 28)
- Targeted spy satellites w RU tools
- Squad 303
  - First month: 40M messages to RU

Platform Wars

Google Maps
- UA mil: “Thank you Google”

TikTok
- Alternate universe

Twitter
- Restrictions both ways

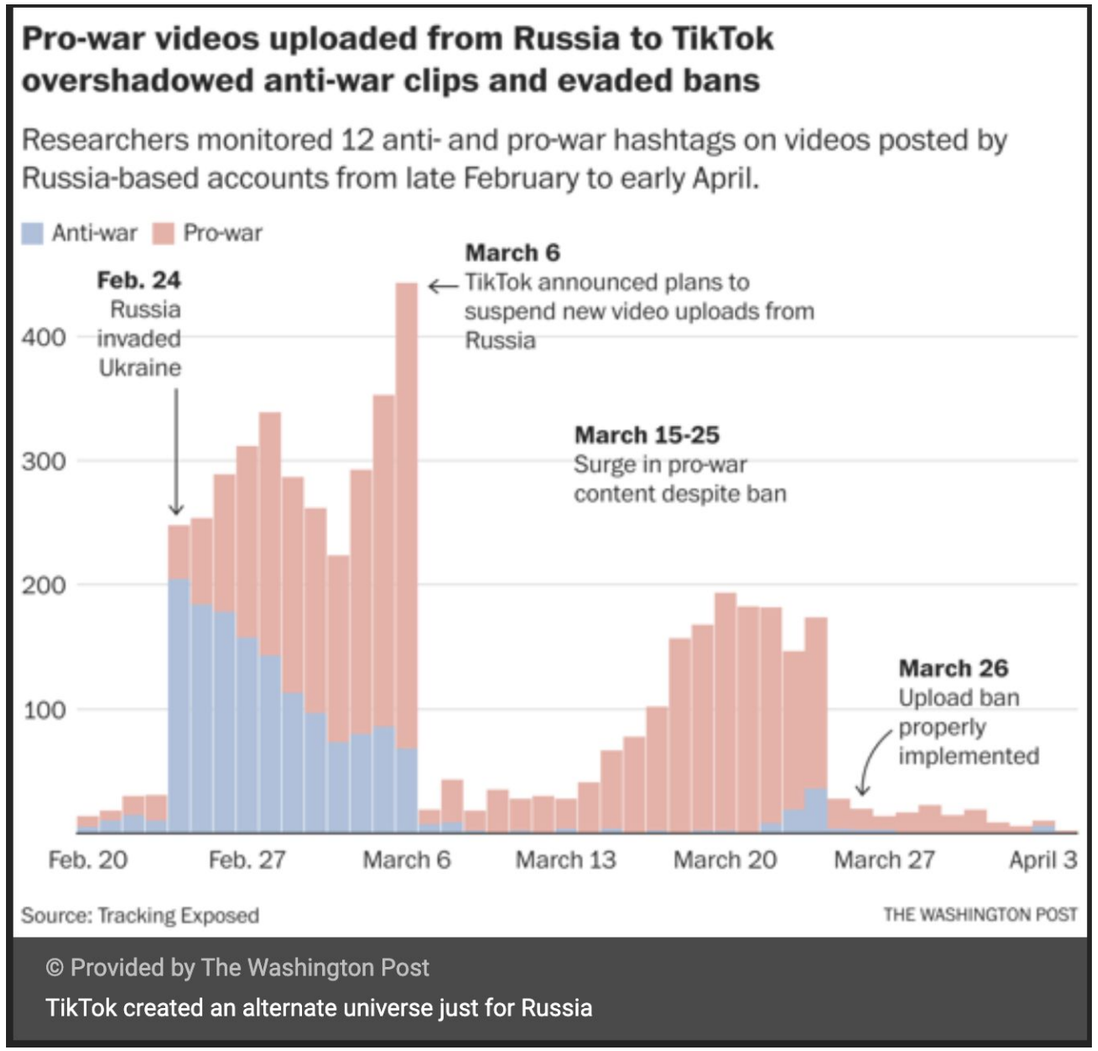
Facebook
- “Extremist”

Instagram
- Still up

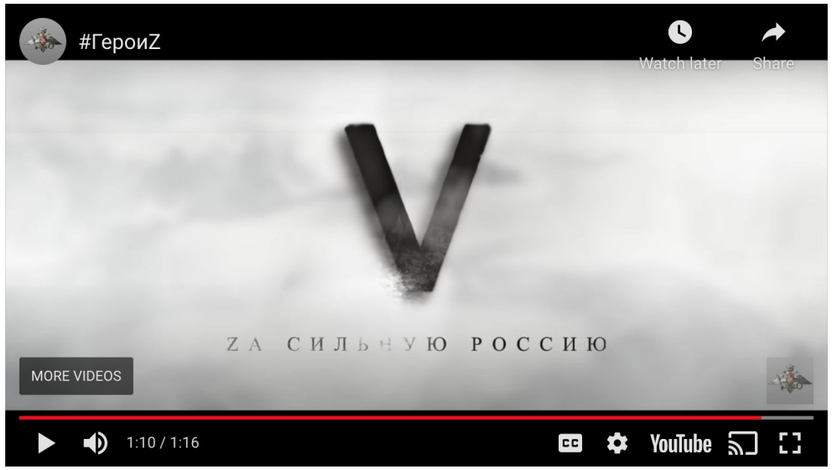
WhatsApp
- Still app

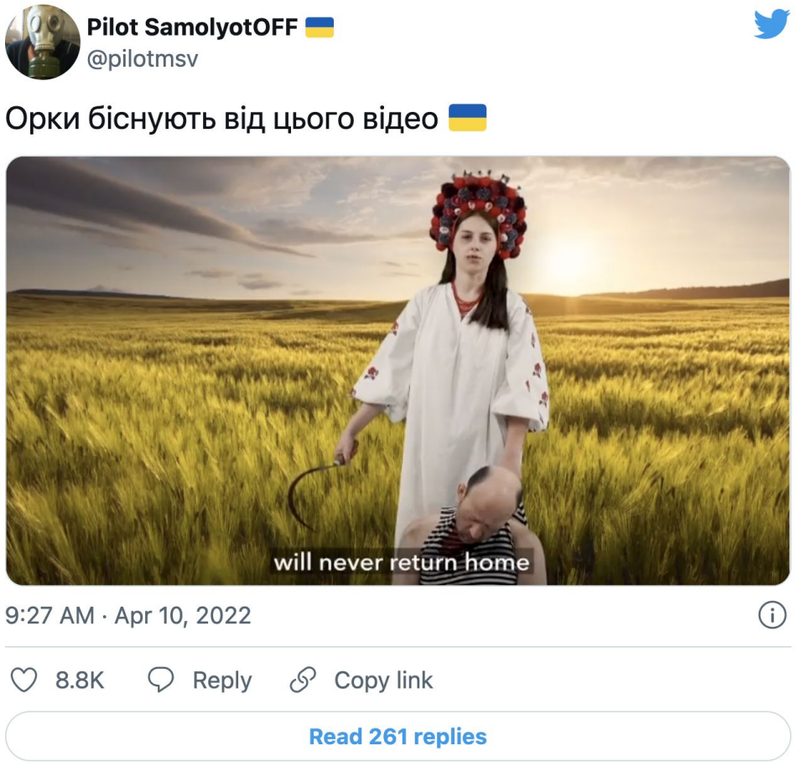
YouTube
- No replacement

Telegram
- Last bastion in Russia



Online Propaganda





RUNET: Digital Iron Curtain

- Far more aggressive since invasion
  - War ≠ war
- RU in UA
  - More access than in RU
  - Banned from social media
  - “Uncomfortable truths”
- Hacker tools vs censorship
- Social media wars
  - Russia vs world
- RU tech industry
  - Brain drain

Online Platform Feature Restrictions by ISP, Russia - RU, 2022-03-13 UTC

asn	asn_name	isp_name	Feature	Platform	Status	reachability ▲	failure_rate
AS39435	EVOLGOGRAD-AS, RU	ER-Telecom	Backend	Instagram	DOWN	0%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Backend	Instagram	DOWN	0%	
AS51645	IRKUTSK-AS, RU	ER-Telecom	OpenGraph	Instagram	DOWN	0%	
AS39435	EVOLGOGRAD-AS, RU	ER-Telecom	Static CDN	Instagram	DOWN	0%	
AS39435	EVOLGOGRAD-AS, RU	ER-Telecom	OpenGraph	Instagram	DOWN	0%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Static CDN	Instagram	DOWN	0%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	Website	Instagram	DOWN	0%	
AS12389	ROSTELECOM-AS, RU	Rostelecom	OpenGraph	Instagram	DOWN	0%	
AS39435	EVOLGOGRAD-AS, RU	ER-Telecom	Website	Instagram	DOWN	0%	
AS31133	MF-MGSM-AS PJSC MegaFon, RU	MegaFon	Static CDN	Instagram	DOWN	0%	
AS51645	IRKUTSK-AS, RU	ER-Telecom	Website	Instagram	DOWN	0%	
AS8402	CORBINA-AS OJSC Vimpelcom, RU	Beeline	OpenGraph	Instagram	DOWN	25%	
AS8402	CORBINA-AS OJSC Vimpelcom, RU	Beeline	Website	Instagram	DOWN	33%	
AS8402	CORBINA-AS OJSC Vimpelcom, RU	Beeline	Static CDN	Instagram	DOWN	40%	
AS8402	CORBINA-AS OJSC Vimpelcom, RU	Beeline	Backend	Instagram	indeterminate	50%	
AS51645	IRKUTSK-AS, RU	ER-Telecom	Static CDN	Instagram	indeterminate	50%	

NETBLOCKS.ORG MAPPING INTERNET FREEDOM

Cyber Allies

NATO Strategy

Cyberspace
- Domain of military operations

Cybersecurity
- “Core task” of collective defense

International law
- Applies in cyberspace

Goal
- Secure, norms-based cyberspace

Strengths
- Diversity & defensive philosophy

Strategic partner
- European Union

NATO Tactics

Cyber Defense Pledge

Defend networks, missions, operations

Integration of national cyber contributions

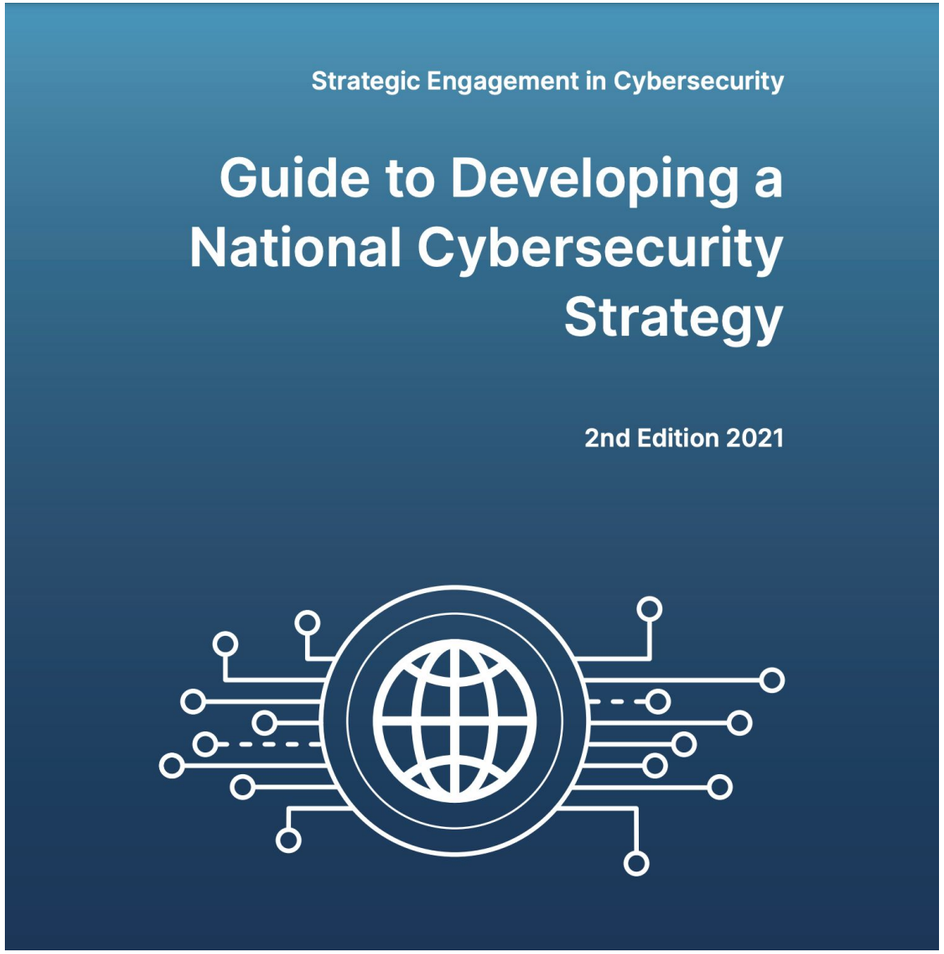
NATO Cyberspace Operations Centre

NATO Industry Cyber Partnership

Malware Information Sharing Platform

National Cybersecurity Strategy

1. **Governance**
   Authority, budget, plan
2. **Risk Management**
   Threat assessment, methodology, policies
3. **Preparedness, Resilience**
   Info sharing, incident response, crisis mgt
4. **Critical Infrastructure, Essential Services**
   Governance, baselines, public-private partnership
5. **Capability, Capacity Building, Awareness**
   Curricula, training, innovation, R&D
6. **Legislation, Regulation, Law Enforcement**
   Legal framework, human rights, compliance
7. **International Cooperation**
   Foreign policy alignment



https://ccdcoe.org/uploads/2022/02/2021-NCS-Guide.pdf

MAY 12-13
BRIEFINGS

The Virtual Battlefield in 2022:
Russia-Ukraine War & Its Policy Implications

Kenneth Geers
Very Good Security