Cyber War in Perspective: Analysis from the Crisis in Ukraine

Kenneth Geers / Comodo
NATO CCD COE / Atlantic Council / DSI-Berlin / TSN Univ Kyiv
Ukraine
Revolution: Humans
Russian reaction: invasion, annexation
NATO CCD COE research

- **Cyber dimension** of conflict
- Ukraine / Russia
  - Necessary ingredients
    - Geopolitical stakes
    - IT / hacking expertise
- Malware: espionage / crime
- **Skeptics**: no cyber war
- International norms
  - Limits to state hacking
  - Tallinn Manual
Cyber attacks present a clear challenge to the security of the Alliance.

Could be as harmful to modern societies as a conventional attack.

Cyber defence is part of NATO’s core task of collective defence.

We ... recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.
US Army FM 3-38: Electromagnetic Cyber Activities

- project power, apply force through cyberspace
- deny, deceive, degrade, destroy, disrupt, [betray]
- enemy / adversary -> activity / capabilities
- may rise to physical damage
- assure access during hostilities
- weapons systems / operator decision-making
- support land objectives (maneuver)
- physical / logical (websites, cyber-persona, IPs)
- within public infrastructure
- comply with the law of war
Cyber War in Perspective - authors

1. Kenneth Geers - CCD COE
2. Keir Giles - CSRC
3. James J. Wirtz - NPS
4. James A. Lewis - CSIS
5. Martin Libicki - RAND
6. Nikolay Koval - CERT UA
7. Glib Pakharenko - ISACA KYIV
8. Jen Weedon - FireEye
9. Tim Maurer - New America
10. Margarita Levin Jaitner - SDU
11. Liisa Past - CCD COE
12. Elina Lange-Ionatamishvili & Sanda Svetoka - STRATCOM COE
13. Nadiya Kostyuk - U Michigan
14. Jan Stinissen - CCD COE
15. Henry Rõigas - CCD COE
17. Jason Healey & Michelle Cantos - Columbia U
18. Richard Bejtlich - Brookings
Free download

Complete book:

Chapters:
https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html

NATO Cyber Defence Library:
https://ccdcoe.org/publication-library.html
CERT UA

- Geopolitical correlation
  - Incidents rise w/ tension
- 2012: defacements
  - UA gov
- 2013: advanced malware
  - Red October, MiniDuke, NetTraveler
- 2014: political doxing
  - UA gov
- Most advanced hack
  - Central Election Commission (CEC)
ISACA Kyiv

- **EuroMaidan**
  - Physical / logical attacks
  - Servers, smartphones, sites, accounts
  - Most serious when shooting started

- **Crimea**
  - Severed network cables, commandeered satellites, mass changes to Wikipedia

- **Eastern Ukraine**
  - Targeting: mobile phone, Wi-Fi
  - Isolation via censorship, forensics
SIGINT + WWW

Ukraine crisis: Transcript of leaked Nuland-Pyatt call

7 February 2014 | Europe

Пайет: Думаю, если ты с ним напрямую свяжешься, это поможет разобраться с ролями всех троих. Также это дает тебе шанс быстро действовать в этой ситуации и обогнать нас. До того, как они ......, и он объяснит, почему ему это не нравится.
Presidental election hack: 25 May 2014

- CyberBerkut vs. Central Election Commission
- Most technically advanced hack (CERT-UA)
- 2+ months recon / Admin access
- Sofacy / APT28 / Sednit malware
- Disabled core CEC nodes
- Possible Cisco ASA zero-day
- Announced “winner” on CEC website
- UA Right Sector boss Dmitry Yarosh
- Broadcast on Russian TV
- Real paper ballots guarantee
Christmas 2015: electricity grid hack

1. Spear phished IT staff
2. VPN credentials to SCADA
3. Backdoor: Black Energy 3
4. Changed passwords
5. Disabled backup power
6. Overwrote firmware: no reconstitution
7. Opened circuit breakers: 3 power distro centers
8. Launched KillDisk via logic bomb
9. 50+ substations offline; 200K+ residents in dark
10. TDoS customer call centers
Прости нас Украина
Military equipment

February 2015
BMP-2 ‘Lavina’
In Uglegorsk, Ukraine
48.311252, 38.288002

August 2014
BMP-2 ‘Lavina’
In Staraya Stanitsa, Russia
48.350068, 40.272248

September 2014
Msta-S in Novoazovsk, Ukraine
47.1275441, 38.0892229

July 2014
Msta-S in Rostov-on-Don, Russia
47.262757, 39.660493
Igor Rosovskiy

- May 2: Odessa fire
- May 3: new Facebook account
  - "local doctor"
- Claims atrocities, anti-semitism
  - Like "fascist occupation"
- 1000s FB, ВКонтакте shares
  - Multiples translations
- Stolen pic: Ruslan Semenov
  - Russian dentist

⚠️ Sorry, this content isn't available right now
Pavel G. Sheremet, 44, who had worked for Russian state television and a pro-Russian outlet in Ukraine, was killed in a car bomb attack in central Kiev on Monday night, Ukrainian authorities said.

Sheremet was a well-known journalist who reported on themes like Russian interference in Ukraine and corruption in the country. His death comes in the wake of an increase in violence and killings of journalists in Ukraine, where the conflict between pro-Russian separatists and the Ukrainian government has left more than 13,000 people dead since 2014.

Sheremet was the editor-in-chief of the Kiev-based newspaper Kiev Post and a contributor to the website of the Russian state television channel RT. He was also a vocal critic of Russian President Vladimir Putin's policies in Ukraine.

The car bomb exploded in front of Sheremet's house, which is located in a residential area of the city. It is not clear who was behind the attack or what motive motivated it.

Sheremet's death has sparked outrage and condemnation from both the Ukrainian government and international leaders.

President Volodymyr Zelensky said in a statement that Sheremet was a “brave and courageous man” who was a “symbol of freedom of speech in Ukraine.”

US Ambassador to Ukraine Marshall Billingslea called Sheremet’s death a “disgraceful act” and said that the United States was “deeply concerned” by the attack.

The International Organization for Journalists said in a statement that it was “shocked and saddened” by Sheremet’s death and called for an investigation into the attack and for those responsible to be held accountable.

Sheremet’s death comes just days after the murder of another Ukrainian journalist, Vitalii Shabun, who was killed in a drive-by shooting in the city of Lutsk.

In recent years, Ukraine has seen a surge in violence against journalists, with more than 100 media workers killed or injured since 2014.

The Ukrainian government has repeatedly denied accusations by the international community that pro-Russian separatists are behind the attacks on journalists.

However, many journalists and human rights activists believe that the attacks are a form of intimidation and censorship, aimed at silencing criticism of the government and its policies.

Sheremet’s death is likely to fuel tensions between Ukraine and Russia, which have been on the rise in recent months due to disputes over the annexation of Crimea and the conflict in eastern Ukraine.

The Ukrainian government has accused Russia of seeking to destabilize the region and has accused Moscow of providing support to separatist groups in eastern Ukraine.

Sheremet was known for his reporting on these issues and had been a vocal critic of Russian interference in Ukraine.

The Ukrainian government has vowed to investigate the attack on Sheremet and to bring those responsible to justice.

However, Sheremet’s colleagues and friends have called for the international community to take action to protect journalists and to hold the responsible parties accountable for the attacks.

They have urged countries to support Ukraine in its efforts to protect the media and to ensure freedom of speech and expression.

Sheremet is survived by his wife and two children.

**Editor’s note:** The article has been updated on July 21 with additional details.
Cyber War in Perspective

- CND -> CNO -> CNE -> CNA
  - Espionage / Sabotage / PSYOP
- Evolution
  - Estonia 2007
    - Availability
  - Ukraine 2014
    - Integrity
  - USA 2016
    - Confidentiality
CYBERCOM: Cyber Analogies Project

- Cyber war
  - Yes it exists
  - But likely not decisive
- Strategy / tactics
  - Can win individual battles
  - May gain time and space
- ADM Yamamoto
  - No WW2 victory at Pearl Harbor
  - Adversary will respond
  - Attacker beware
National security challenges

- Defense: connectivity, vulnerability
- Attack: peacetime limits?
- Intent: CNE or CNA?
- Deterrence: proactive, reactive
- Security dilemma
- Retaliation: laws of war
- Critical infrastructure: Big Brother
- Arms control: prohibition, inspection
- Policy / law: tech too fast
- Attribution: SECRET (crowdsourse?)
Cyber War in Perspective: Analysis from the Crisis in Ukraine

Kenneth Geers / Comodo
NATO CCD COE / Atlantic Council / DSI-Berlin / TSN Univ Kyiv
Ukraine