Cyber War in Perspective:
Analysis from the Crisis in Ukraine

Kenneth Geers / Comodo

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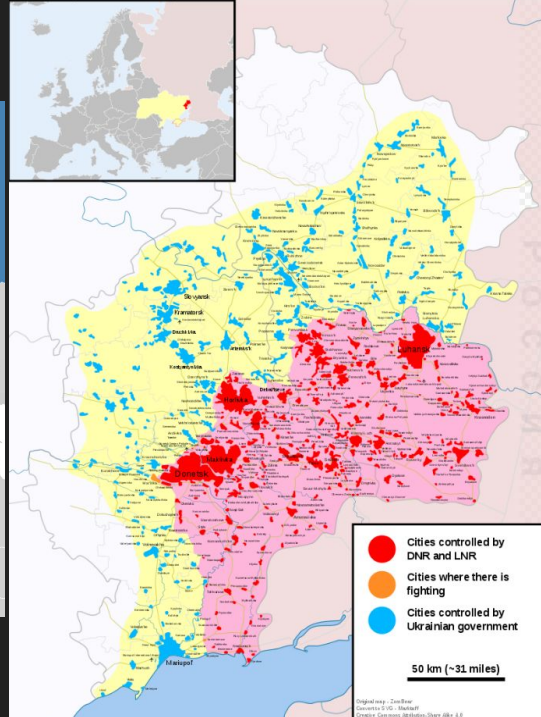
Ukraine

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

NATO Warsaw Summit Communiqué - July 2016

- 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

FM 3-38
CYBER
ELECTROMAGNETIC
ACTIVITIES

FEBRUARY 2014
DISTRIBUTION RESTRICTION:
Approved for public release; distribution is unlimited.
HEADQUARTERS, DEPARTMENT OF THE ARMY
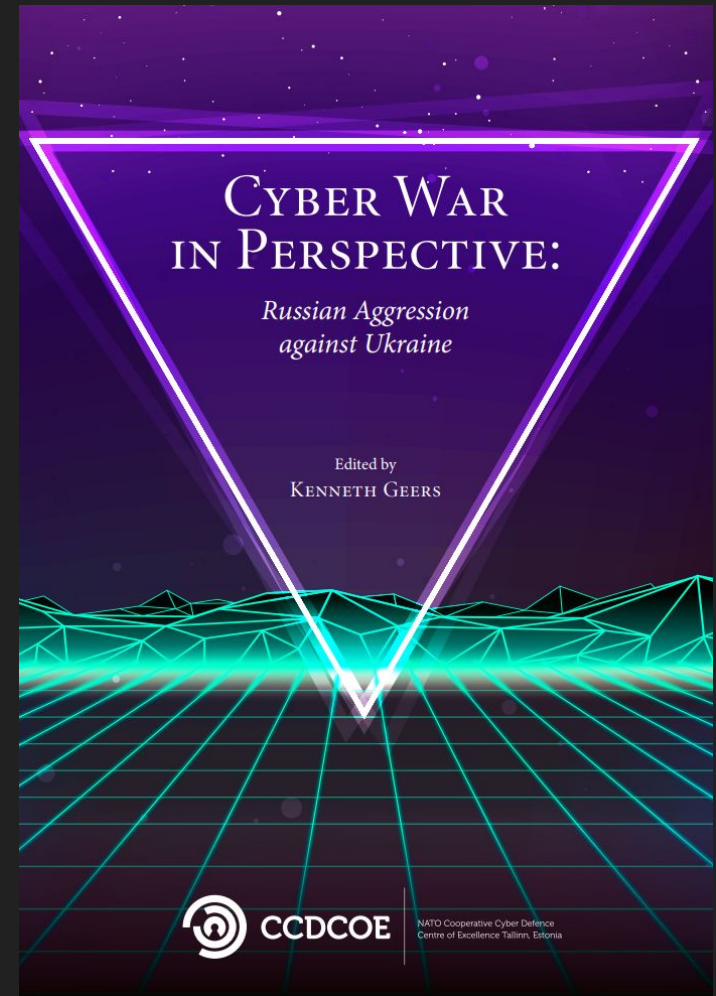
Cyber War in Perspective: authors

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
16. Jarno Limnéll - Aalto U
17. Jason Healey & Michelle Cantos - Columbia U
18. Richard Bejtlich - Brookings

Free book download

Volume: https://ccdcoe.
org/sites/default/files/multimedia/pdf/CyberWar
inPerspective_full_book.pdf

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)

CERT-UA
CERT-UA
Computer Emergency
Response Team of Ukraine

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

ISACA®
Trust in, and value from, information systems

SIGINT + WWW

Ukraine crisis: Transcript of leaked Nuland-Pyatt call

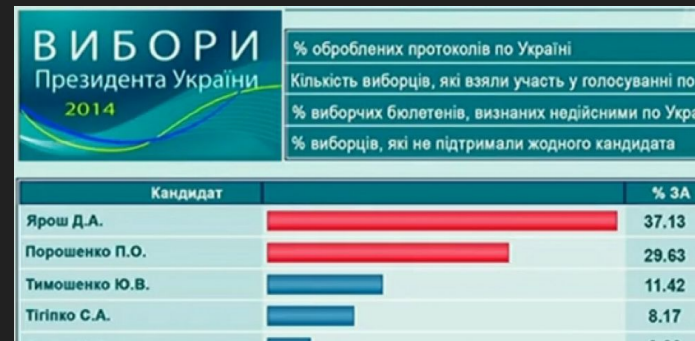7 February 2014 | Europe

BBC

You Tube UA   Search

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.

Presidential 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

КИБЕРБЕРКУТ
МЫ НЕ ЗАБУДЕМ • МЫ НЕ ПРОСТИМ

ВИБОРИ
Президента України
2014

	% оброблених протоколів по Україні
	Кількість виборців, які взяли участь у голосуванні по
	% виборчих бюлетенів, визнаних недійсними по Укра
	% виборців, які не підтримали жодного кандидата

Кандидат	% ЗА
Ярош Д.А.	37.13
Порошенко П.О.	29.63
Тимошенко Ю.В.	11.42
Тігіпко С.А.	8.17

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
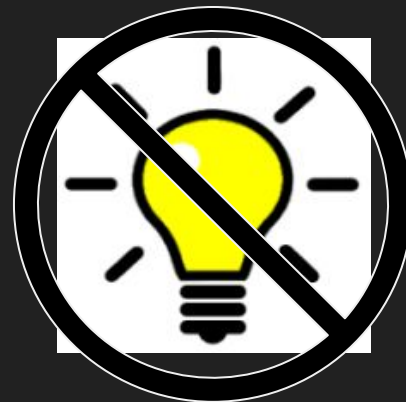
Russian e-billboard

0:36 / 1:07

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

LUHANSK

DONETSK

BORDER BETWEEN UKRAINE
AND THE RUSSIAN FEDERATION

MARIUPOL

Social Media

VICE NEWS

14:42

23:13

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

Здравствуйте, меня зовут Игорь Розовский, мне 39 лет, я живу в городе Одессе. В течении 15 лет я работаю врачом в службе скорой помощи. Вчера, как вы знаете, в нашем города случилась страшная трагедия, одни люди убили других. Убили жестоко - сожгли живыми. Не в состоянии опьянения, не за наследство бабушки, а потому что они не разделяют политических взглядов националистов. Сначала жестоко избивали, потом жгли.
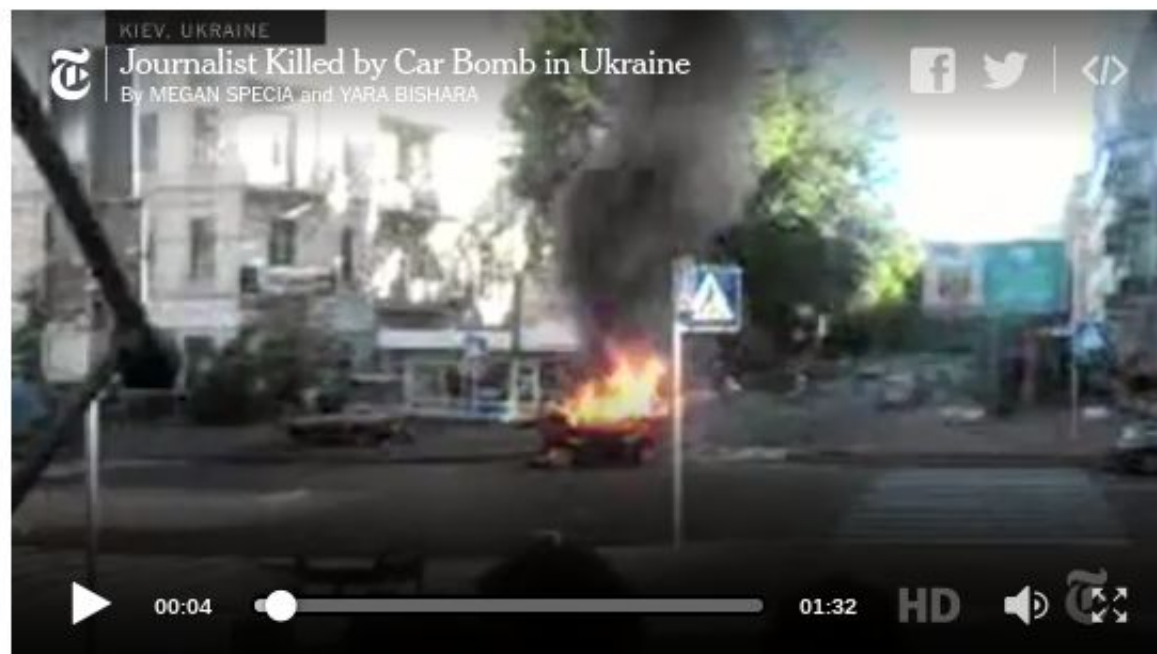Как врач я поспешил оказать помощь тем, кого можно было спасти, но меня остановили боевики, не дав подойти к раненому. Один из них грубо оттолкнул меня, пообещав, что скоро меня и других евреев Одессы ждет такая же участь.
Я видел парня, которого можно было спасти, если бы я смог забрать его в больницу, но все уговоры закончились ударом по моему лицу и потерей очков.

Pavel Sheremet, Journalist in Ukraine, Is Killed in Car Bombing

By ANDREW E. KRAMER   JULY 20, 2016

KIEV, UKRAINE

Journalist Killed by Car Bomb in Ukraine
By MEGAN SPECIA and YARA BISHARA

00:04   01:32   HD

Pavel G. Sheremet, 44, who had worked for Russian state

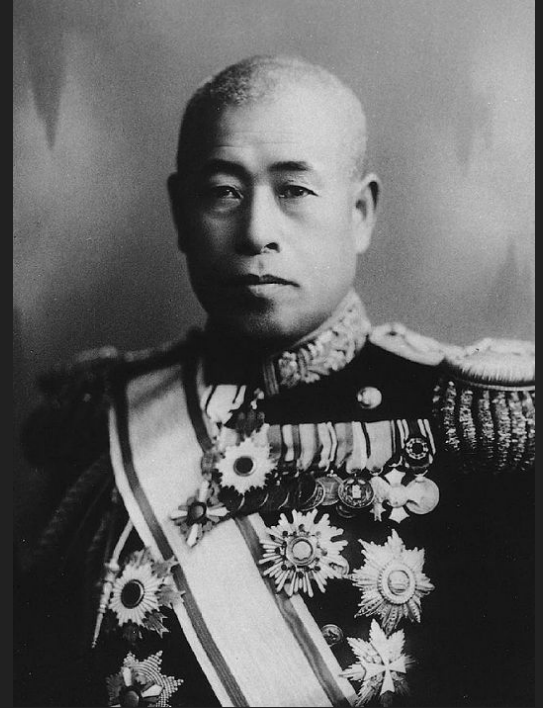# As Democrats Gather, a Russian Subplot Raises Intrigue

By DAVID E. SANGER and NICOLE PERLROTH   JULY 24, 2016

Vladimir V. Putin in Moscow last month. Democratic leaders and cyberspecialists wonder if Mr. Putin is meddling in the presidential election. Pool photo by Ivan Sekretarev

Summary

- Cyber war exists
  - Espionage / sabotage
  - Estonia 2007: availability
  - Ukraine 201X: integrity
- Cyber war unlikely to be decisive
  - Can win individual battles
  - May gain time and space
- ADM Yamamoto
  - No WW2 victory at Pearl Harbor
  - Adversary will respond
  - Attacker beware

Cyber War in Perspective:
Analysis from the Crisis in Ukraine

Kenneth Geers / Comodo

NATO CCD COE / Atlantic Council / DSI-Berlin / TSN Univ Kyiv

Ukraine