# The future and cyber warfare?

BG Paul Ducheine & COL Peter Pijpers
Netherlands Defence Academy – University of Amsterdam

1

## Prediction (2017)

"The next war will take place in cyberspace!"


PD, in : KIJK 2017

2

## Astonishment (2022, Mar 6)

"Why haven't we seen hard cyber operations by Russian and Ukrainian armed forces (yet)?


PD on LinkedIn:
bit.ly/3VwNLfb
Twitter thread: @PaulDucheine

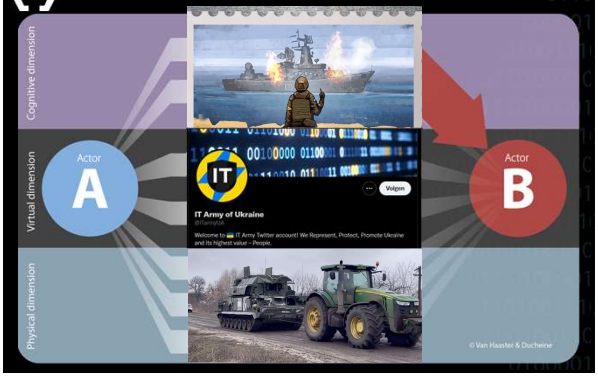
3

## Topics

1. War in '3D'
2. Conflict in 3D + all instruments of power
3. Cyberspace & operations
4. Observations
5. Conclusion

4

## 1. War in 3D: 3 dimensions



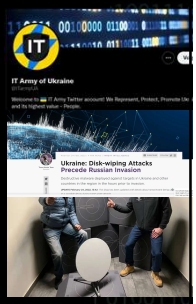


5

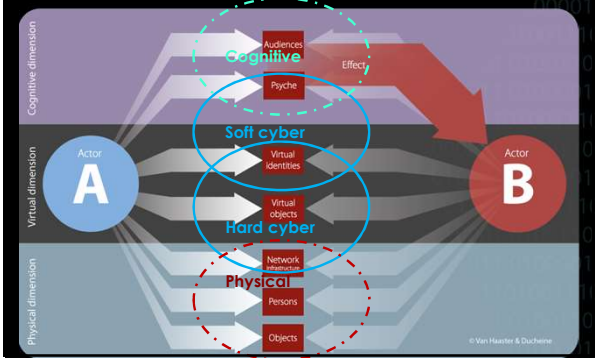
## 3. Cyberspace

'all entities … digitally … connected'

- People (cognition)
- Virtual identities
- Virtual objects
  - Software
    - Protocols, Firmware, Operating Systems, Applications, etc.
  - Data/content
- Hardware
- Objects
- Persons (body)
- Geographical locations




## 3. Operations




## Zelensky

**Boris Johnson and Volodymyr Zelensky walked through the center of Kiev, taking the locals by surprise**

April 9, 2022 in World 0

16

## Q&A Spoiler

"The next war will take place in cyberspace!"?

- Indeed, it does, but ….
  …. in another way (TBC).
- However, although there's a <u>war</u> in cyberspace, ….
  …. there's even more <u>conflict</u> in cyberspace.

20

## Topics

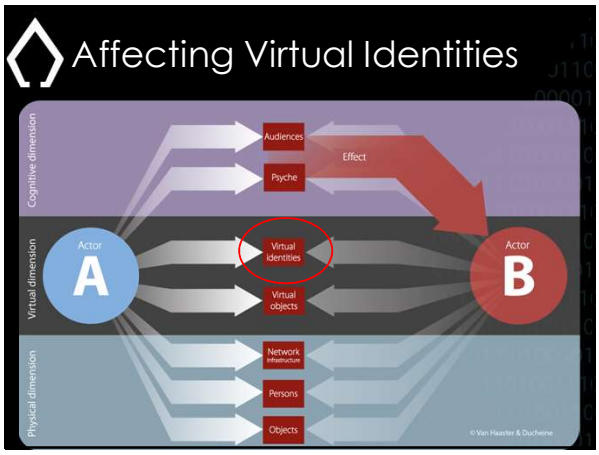
1. War in '3D'
2. Conflict in 3D + all instruments of power
3. Cyberspace & operations
4. Observations
   a. Hard cyber operations ('hacken')
   b. Soft cyber operations ('influencing')
   c. IT-services & IT-infra
   d. (H)activists
5. Conclusion

21

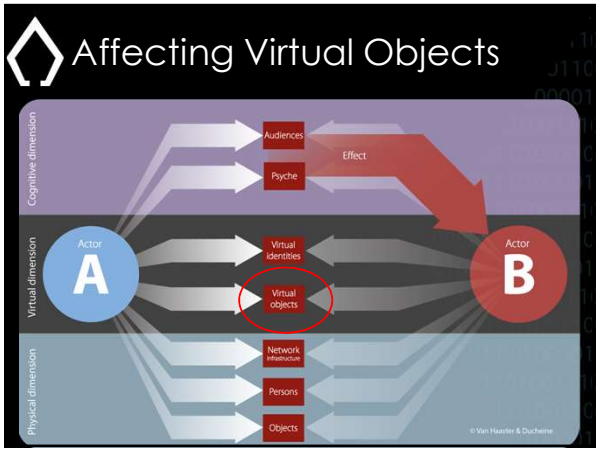
## 4a. Hard cyber operations

- Caveats:
  - Info limited (open sources)
  - Identity 'author' unclear (attribution)
    - RF / UA, proxies, hactivists
- Operations (i.a.):
  - Limited (not executed)? …. Because?
  - Or?
  - Executed, but …..

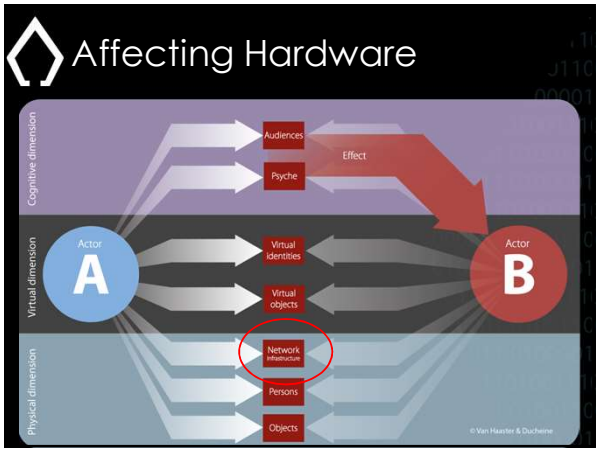
24

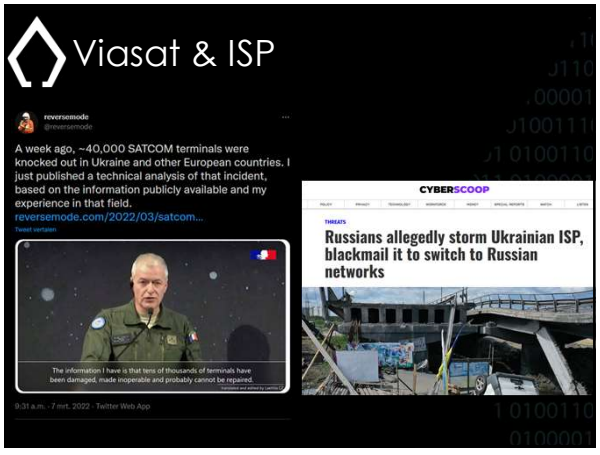

Affecting Virtual Identities
Cognitive dimension
Virtual dimension
Physical dimension
Audiences
Psyche
Effect
Actor A
Actor B
Virtual identities
Virtual objects
Network infrastructure
Persons
Objects
© Van Haaster & Ducheine


Home » Technology » Twitter: Ukrainian accounts compromised by Russian hackers
Twitter: Ukrainian accounts compromised by Russian hackers
by world today news February 25, 2022
No Comments
IT Army of Ukraine
@ITarmyUA
Welcome to IT Army Twitter account! We Represent, Protect, Promote Ukraine and its highest value – People.
Volgen
IT Army of Ukraine @ITarmyUA · 1 mrt.
Took offline rial_bru, Russia's largest source of propaganda news.
#TangoDown #Ukraine #RussiaUkraine #Anonymous


Affecting Virtual Objects
Cognitive dimension
Virtual dimension
Physical dimension
Audiences
Psyche
Effect
Actor A
Actor B
Virtual identities
Virtual objects
Network infrastructure
Persons
Objects
© Van Haaster & Ducheine


Ukraine: Disk-wiping Attacks Precede Russian Invasion
Destructive malware deployed against targets in Ukraine and other countries in the region in the hours prior to invasion.
UPDATE February 24, 2022, 13:42:
Code-signing certificate issued
2021-04-13
Oldest known IsaacWiper sample compiled
2021-10-19
Oldest known HermeticWiper sample compiled
2021-12-28
Mass deployment of HermeticWiper in Ukraine
2022-02-23
IsaacWiper deployed in Ukraine
Code-signing certificate revoked
2022-02-24


Affecting Hardware
Cognitive dimension
Virtual dimension
Physical dimension
Audiences
Psyche
Effect
Actor A
Actor B
Virtual identities
Virtual objects
Network infrastructure
Persons
Objects
© Van Haaster & Ducheine

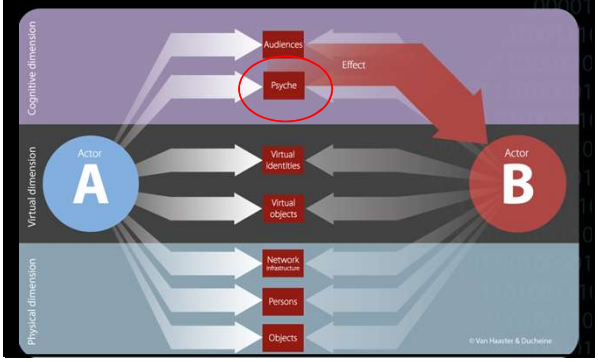

Viasat & ISP
reversemode
@reversemode
A week ago, ~40,000 SATCOM terminals were knocked out in Ukraine and other European countries. I just published a technical analysis of that incident, based on the information publicly available and my experience in that field.
reversemode.com/2022/03/satcom...
The information I have is that tens of thousands of terminals have been damaged, made inoperable and probably cannot be repaired.
9:31 a.m. · 7 mrt. 2022 · Twitter Web App
CYBERSCOOP
THREATS
Russians allegedly storm Ukrainian ISP, blackmail it to switch to Russian networks

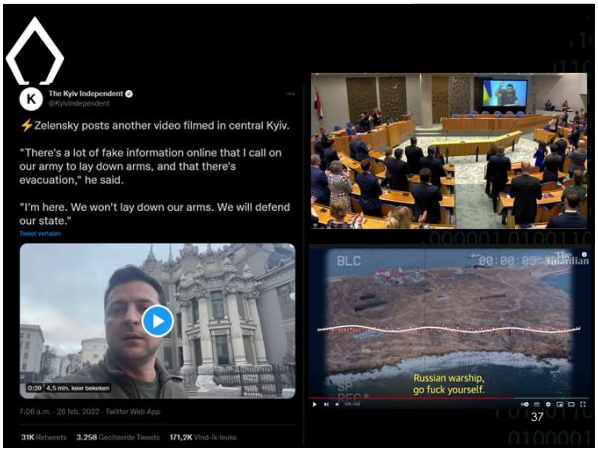
## 4b. Soft Cyber Operations

- Both sides:
  - Armed forces, RF, UA, proxies, activists
- Goal: influencing audience
  - Deception
  - False flag etc.
  - Recruiting (IT-Army of Ukraine)
  - Propaganda (Zelensky, Poetin)
  - Public support (Snake Island)
  - Int'l public support (Fedorov)
  - Hack & Leak

35

## Affecting 'Psyche'




37

## 4c. IT-services & IT-infra

- Motives:
  - Restrictions (EU-sanctions; RF-law)
  - Commercial (Starlink)
  - Ideological (Microsoft, Allies)
  - Neutral (ICANN, RIPE)
- Examples
  - Work around (Twitter via TOR)
  - Cyber threat intell & -security (Microsoft)
  - <Broadband (Lumen, Cogent)
  - Relocating service/infra (Cloudflare)
  - Withdrawal (PayPal, Apple-stores)

38

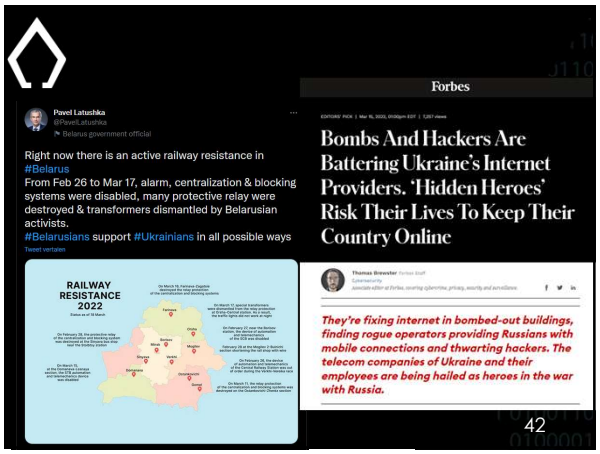
## IT services



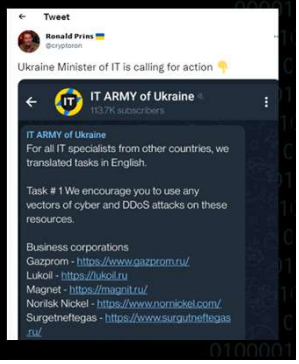
## 4d. (H)activism

- Who:
  - Proxies?
  - Anonymous, IT Armies, etc.
  - Coordination, accountability
- How:
  - Bounty program (bugs) > DDoS etc.
  - Hacking (i.a. ICS Belarus Railway)
  - Cancelling firms
  - Hack & Leak
  - Censor work arounds :
    - Google Reviews / Tripadvisor
    - TOR-Twitter

41




42


## 5. Conclusions

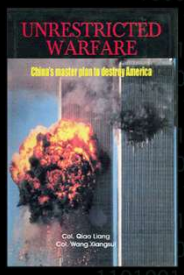
- War in 3 dimensions, incl. virtual
  - Synchronisation (land, air, cyberspace, EM)
  - Hard: 'War is complicated'
  - Preparation/less visible/defences
- Conflict (in 3D) with DIME
  - Soft: Information, audiences, services
- Proliferation
  - Actors, IT-companies, targets, techniques
- Coordination & accountability?
- 'Unrestrictedness'

46

## 'Unrestricted Warfare' (1999)

'Unrestricted':

1. Means
2. Medium/Vector
3. Addressees (Target)
4. Locus
5. Rules (of Engagement)
6. Conventions:
   political, economic, cognitive
   (disrupt, deceive, surprise)




48