Hacking the Hackers: Strategic Analysis in Cyber Defense

Kenneth Geers

Senior Research Scientist, Comodo

NATO Cyber Centre, Atlantic Council,

Digital Society Institute-Berlin, TSN University of Kyiv

Peloponnesian War

Athens: sea power

Sparta: land power

Why do we fight?

When is it over?

USS Cole

National security

Network security

Cyber security

Strategic Trends

Code

Net

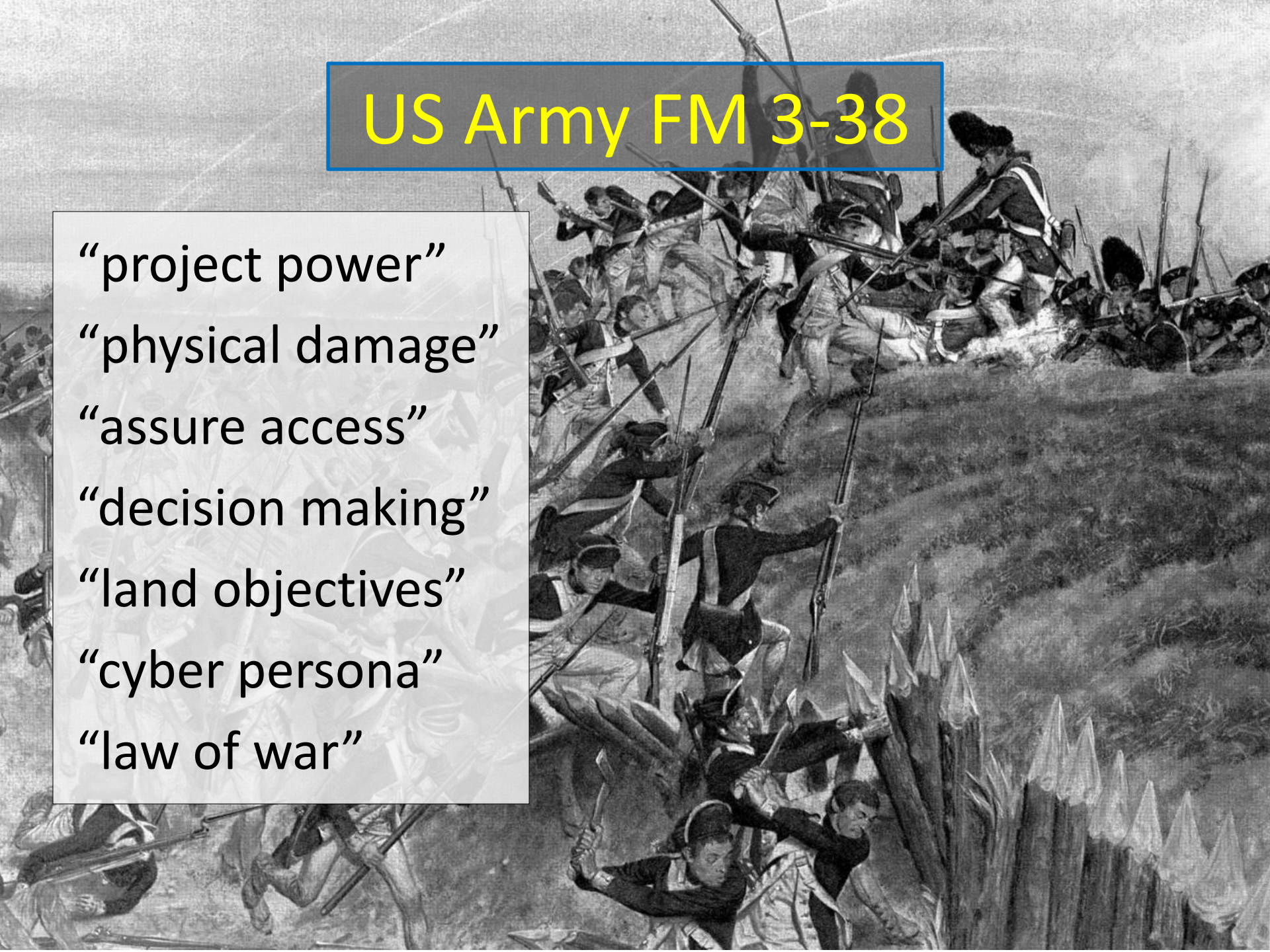
Drones

Robots

AI

Ethics

US Army FM 3-38



"project power"

"physical damage"

"assure access"

"decision making"

"land objectives"

"cyber persona"

"law of war"

Israel: cyber

"relentless"

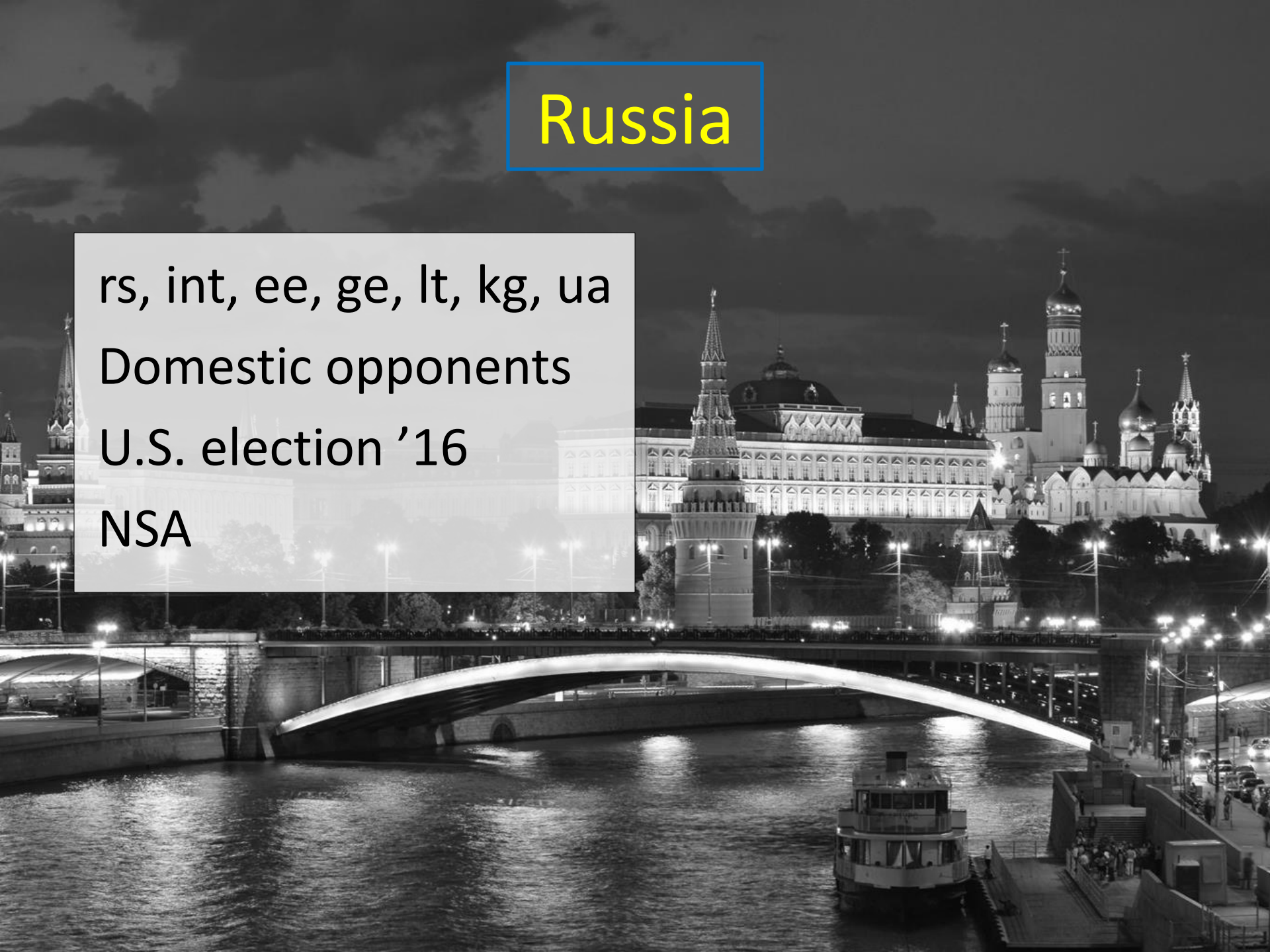
"at all fronts"

"enemy projects"

"public opinion"

"war and peace"

Ukraine
Military
Politics
Diplomacy
Infrastructure
Business
Social media
СЛУЦЬК
СУРАЖ
МГЛИН
ПОЧЕП
СТАРОДУБ
ТРУБЧЕВСЬК
БРЕСТ-ЛИТОВСЬК
ПІНСЬК
ПОЛІСЬКА
МОЗИР
ОКРУГА
ДУБРОВНИЦЯ
ЧЕРНІГІВ
ЧЕРНІГІВСЬКА
СІВЕРСЬКИЙ
ГЛУХІВ
РИЛЬСК
СОСНИЦЯ
ПУТИВЛЬ
ГУБЕРНІЯ
КОНОТОП
СУМИ
СУДЖА
НІЖИН
КИЇВ
РОМНИ
ПРИЛУКИ
ОХТИРКА
ХАРКІВ
ВОВЧАНСЬК
ГРАЙВОРОН
БІЛГОРОД
ОБУХІВ
ПЕРЕЯСЛАВ
ЛУБНИ
МИРГОРОД
БОГОДУХІВ
КУП'ЯНСЬК
КАНІВ
ПОЛТАВСЬКА
ПОЛТАВА
ЗМІЇВ
ХАРКІВСЬКА
СТАРОБІЛЬСЬК
БІЛА ЦЕРКВА
ЗОЛОТОНОША
ІЗЮМ
ТАРАЩА
ЧЕРКАСИ
КОНСТЯНТИНОГРАД
КРЕМЕНЧУК
ЧИГИРИН
ЗВЕНИГОРОДКА
НОВОМОСКОВСЬК
ПАВЛОГРАД
БАХМУТ
ЛУГАНСЬК
ОЛЕКСАНДРІЯ
ДЕБАЛЬЦЕВЕ
УМАНЬ
ВЕРХНЬОДНІПРОВСЬК
ЄЛИЗАВЕТГРАД
КАТЕРИНОСЛАВ
ЮЗІВКА
ОЛЕКСАНДРІВСЬК
ГУЛЯЙПОЛЕ
КРИВИЙ РІГ
НІКОПОЛЬ
АНАНЬЇВ
ХЕРСОНСЬКА
МАРІУПОЛЬ
ТАВРІЙСЬКА
БЕРДЯНСЬК
МИКОЛАЇВ
МЕЛІТОПОЛЬ
ТИРАСПОЛЬ
ХЕРСОН
ЄЙСЬК
БЕНДЕРИ
ОДЕСА
ПЕРЕКОП
СЛОВ'ЯНСЬКА
КЕРЧ
ТЕМРЮК
СІМФЕРОПОЛЬ
БАХЧИСАРАЙ
НОВОРОСІЙСЬК
ГАЛАЦ
ІЗМАЇЛ
БРАШОВ
СІБІУ
ЛЬВІВ
ТЕРНОПІЛЬ
ІВАНО-ФРАНКІВСЬК
ЧЕРНІВЦІ
ЖИТОМИР
ВІННИЦЯ
ЛУЦЬК
РІВНЕ
ВОРОНІЖ
КУРСЬК
ЛЬГОВ
СТАРИЙ ОСКІЛ
БОБРОВ
КОРОЧА
НОВИЙ ОСКІЛ
ВАЙЛУКИ
РОЗСОШ
БОГУЧАР
УРЮПІНСЬКА
РОСТОВ
ТАГАНРІГ
НОВОЧЕРКА
УМАНСЬКА



Russia

rs, int, ee, ge, lt, kg, ua

Domestic opponents

U.S. election ’16

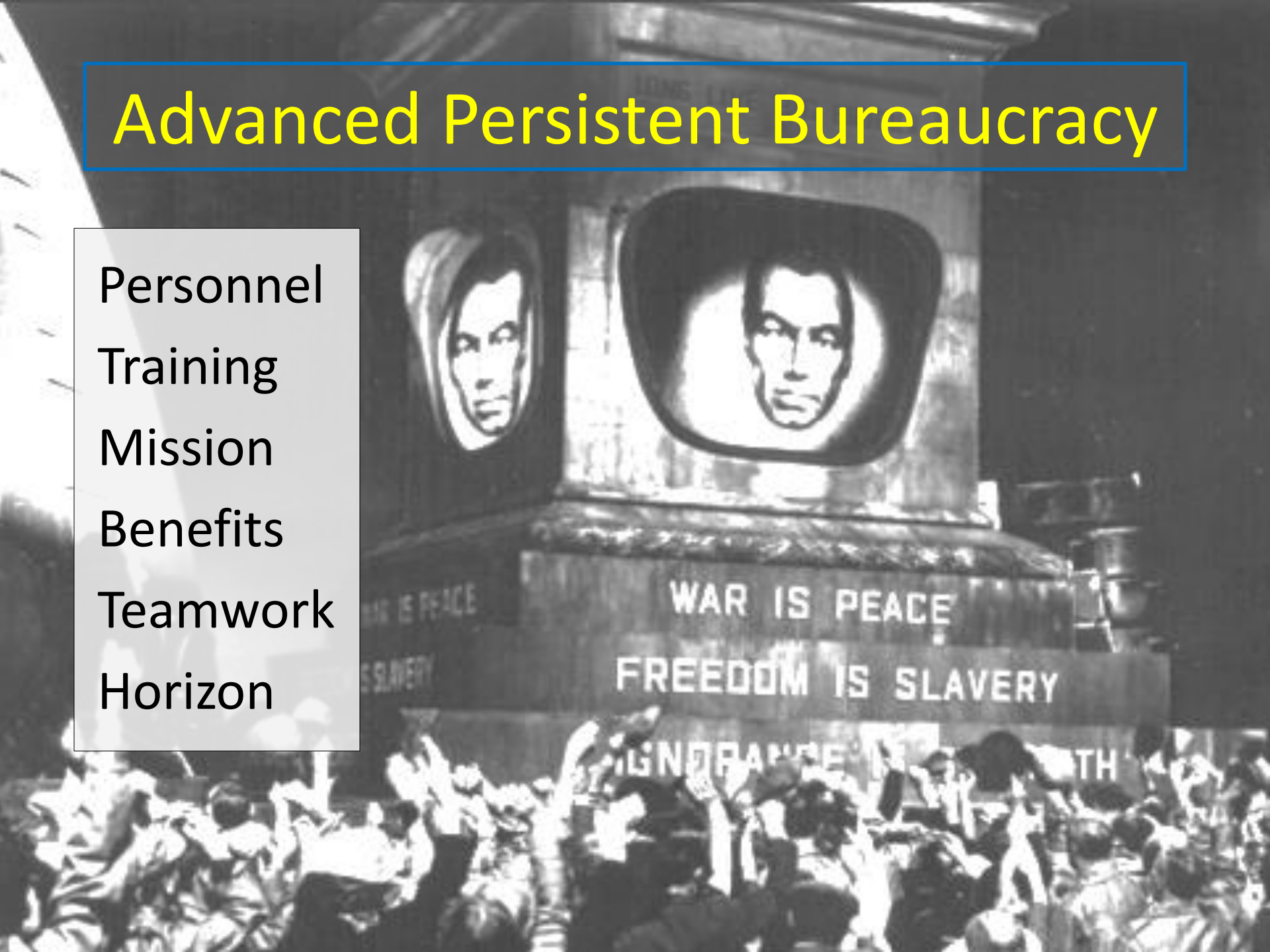
NSA

NATO
“clear challenge”
“harmful as conventional”
“core task”
“domain of operations”

Strategic Analysis

- Position
- Perspective
- Patterns
- Plans
- Ploys

Advanced Persistent Bureaucracy



- Personnel
- Training
- Mission
- Benefits
- Teamwork
- Horizon

Crowdsourcing

www = best defense

Distributed analysis

Curiosity

Puzzle solving

Teamwork

Cyber Security Firms

www = best intelligence

No chain of command

Corporate competition

Live data

Read!

STXNT
Perimeter 4.7 miles
Belarus
USA
Germany
Hungary
Finland
?
200
meters
0
200

Collaboration

Colleagues
Comrades
Friends

Distant Early Warning

Canada
Greenland
GIUK
Poland
Romania
Undersea
Space

Hacking the Hackers: Strategic Analysis in Cyber Defense

Kenneth Geers

Senior Research Scientist, Comodo

NATO Cyber Centre, Atlantic Council,

Digital Society Institute-Berlin, TSN University of Kyiv