



The Military Role in Cyberspace

Brad Bigelow

Principal Technical Advisor

Deputy Chief of Staff Cyberspace

Supreme Headquarters Allied Powers Europe (SHAPE)

Is Cyber War a Reality?

What Cyber War Is Not

Attack the Internet, Men!



FOREWORD BY PROFESSOR KIM C. BEAZLEY

AUSTRALIA AND CYBER-WARFARE

GARY WATERS, DESMOND BALL, IAN ELDREDGE



GRID ATTACK

CYBER WAR

JAMES ROSONE & MIRANDA WATSON



CYBER WARFARE

AND THE NEW WORLD ORDER

WORLD WAR III SERIES BOOK 4

SECOND EDITION

SURVIVING CYBERWAR

THE EVOLUTION OF CYBER WAR

International Norms for
Emerging-Technology Weapons

BRIAN M. MAZANEC

CYBERDETERRENCE AND CYBERWAR

@WAR THE RISE OF CYBER WARFARE

"CHILLING... EXTRAORDINARY AND URGENT"
WASHINGTON POST

THERE WILL BE CYBERWAR

CYBER- WAR

How Russian Hackers
and Trolls Helped
Elect a President



WHAT WE DON'T, CAN'T, AND DO KNOW

KATHLEEN
HALL JAMIESON

"Eye-opening... a page-turner... consistently surprising."—The New York Times

DARK TERRITORY

THE
SECRET HISTORY
OF
CYBER WAR

FRED KAPLAN

WITH A NEW AFTERWORD BY THE AUTHOR

BRANDON VALERIANO | RYAN C. MANESS

CYBER WAR VERSUS CYBER REALITIES

INTERNATIONAL SYSTEM

21st Century Chinese Cyberwarfare

William T. H.

CYBER WAR

"A harrowing—and persuasive—
picture of the cyberthreat the
United States faces today."
—MICKO KAKUTANI,
NEW YORK TIMES

NEW YORK
TIMES
BESTSELLER

THE NEXT THREAT
TO NATIONAL SECURITY
AND WHAT TO DO ABOUT IT

ENCYCLOPEDIA OF CYBER WARFARE

CYBER WARFARE

How Conflicts in Cyberspace Are Challenging
America and Changing the World

CYBER WAR IN PERSPECTIVE:

Russian Aggression
against Ukraine

THE REAL CYBER WAR

The Political Economy
of Internet Freedom

Shawn M. Powers &
Michael Jablonski

Bundeswehr rüstet sich für den Cyberkrieg

FBI — FLASH ALERT

US Election Databases
HACKED!

Conficker

RANSOMWARE
NotPetya

Globālais kiberkarš jau ir sācies

HACKED

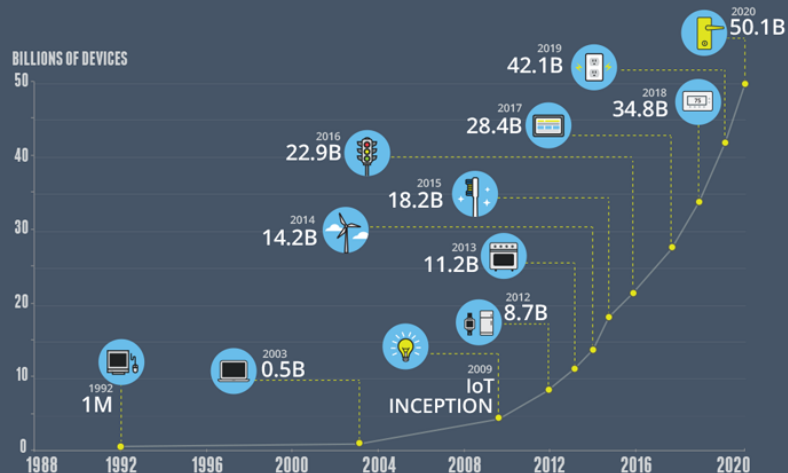
Shadow Brokers, le brouillard de la guerre dans le cyberspace

WannaCry

Wojna w cyberprzestrzeni?

GROWTH IN THE INTERNET OF THINGS

THE NUMBER OF CONNECTED DEVICES WILL EXCEED **50 BILLION** BY 2020



AUG 2017

GLOBAL DIGITAL SNAPSHOT

THE LATEST NUMBERS FOR INTERNET, SOCIAL MEDIA, AND MOBILE USAGE AROUND THE WORLD

TOTAL POPULATION



7.524
BILLION

URBANISATION:
54%

INTERNET USERS



3.819
BILLION

PENETRATION:
51%

ACTIVE SOCIAL MEDIA USERS



3.028
BILLION

PENETRATION:
40%

UNIQUE MOBILE USERS



5.052
BILLION

PENETRATION:
67%

ACTIVE MOBILE SOCIAL USERS



2.780
BILLION

PENETRATION:
37%

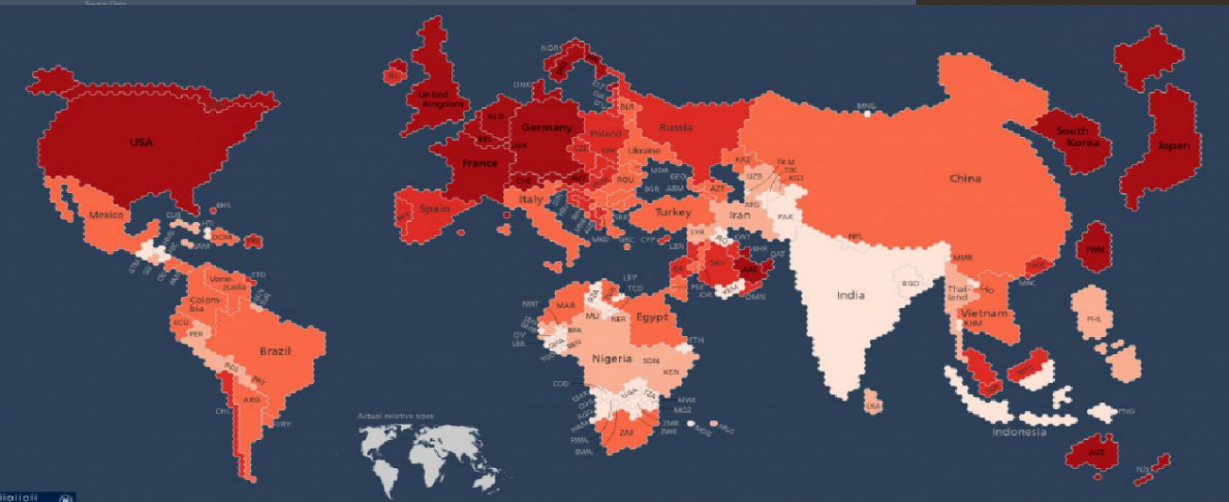
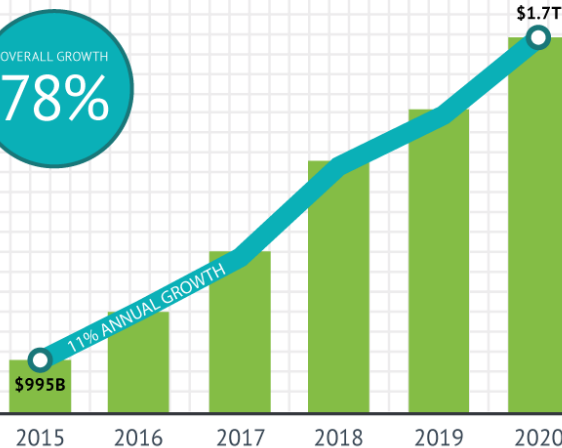


SOURCES: POPULATION: UNITED NATIONS, U.S. CENSUS BUREAU; INTERNET: INTERNET WORLD STATISTICS, IHS; INTERNET USAGE: IHS; WORLD FACTBOOK; FACEBOOK; NATIONAL REGULATORY AUTHORITIES; SOCIAL MEDIA: FACEBOOK, TENCENT, WOXIANG; INTERNET: IHS; KIMCO, NAVIER, NII; AGHAR; CAFERAZZAR; S; SIMILARWEB; DING; EXTRAPOLATION OF TNS



Hootsuite we are.

ECOMMERCE B2C GLOBAL SALES



Our Political

Economic

Social

Personal

Lives

Our Political

Legal

Economic

Commercial

Social

Media

Personal

Military

Lives

Systems

Our Political

Legal

Economic

Commercial

Social

Media

Personal

Military

Lives

Systems

Are Increasingly Dependent Upon Cyberspace

Our Po

Econ

Per



NATO

mercial

a

ary

ms

Cyberspace Defence

IS

A Matter of Collective Defence

Are Incre

cyberspace

Warsaw Summit Communiqué:



Now, in Warsaw, we reaffirm NATO's defensive mandate, and **recognize 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.

This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances.

It will **support NATO's broader deterrence and defence:** cyber defence will continue to be **integrated into operational planning and Alliance operations and missions**, and we will work together to contribute to their success.

Warsaw Summit Communiqué:

Now, in Warsaw, we reaffirm NATO's defensive mandate,

cyberspace as a domain of operations

the air, on land, and at sea.

This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances.

It will **support NATO's broader deterrence and defence:** cyber defence will continue to be **integrated into operational planning and Alliance operations and missions**, and we will work together to contribute to their success.



Warsaw Summit Communiqué:



Now, in Warsaw, we reaffirm NATO's defensive mandate, and **recognize 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.

This will improve NATO's ability to protect and conduct operations across these domains and maintain our freedom of action and decision, in all circumstances.

**integrated into operational planning
and Alliance operations and missions**

missions, and we will work together to contribute to their success.

Straightforward, Right?

Cyberspace as an Operational Domain



**Cyberspace as an
Operational Domain**

=

**Cyberspace as an
Operational Capability**

Lines of Development

	Doctrine
	Organisation
	Training
	Materiel
	Logistics
	Personnel
	Facilities
	Interoperability

Two Fundamental Considerations

1

Integrating Cyberspace into Joint Operations

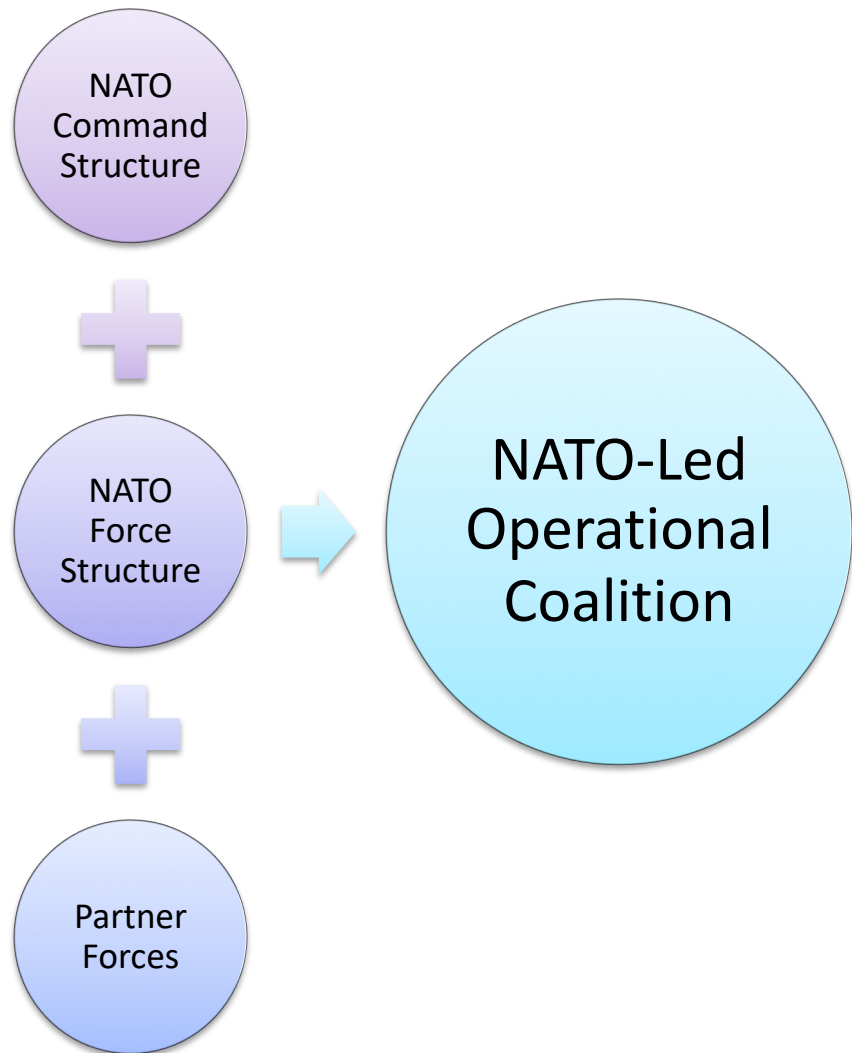
2

Addressing the Unique Aspects of Cyberspace

1

Integrating
with Joint
Operations

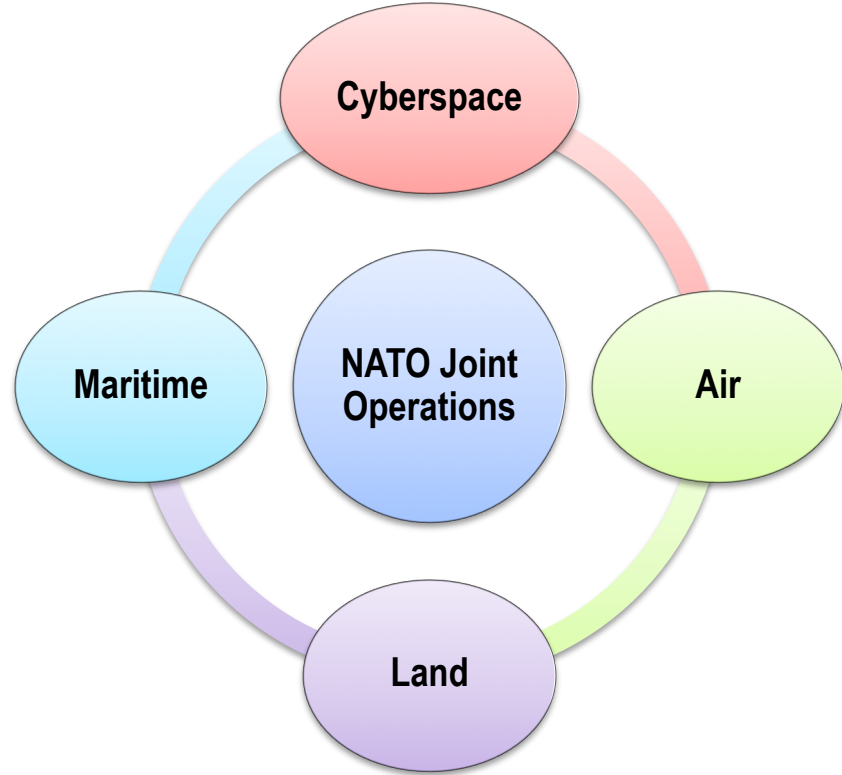
Integration into Effective Coalition Forces



1

Integrating
with Joint
Operations

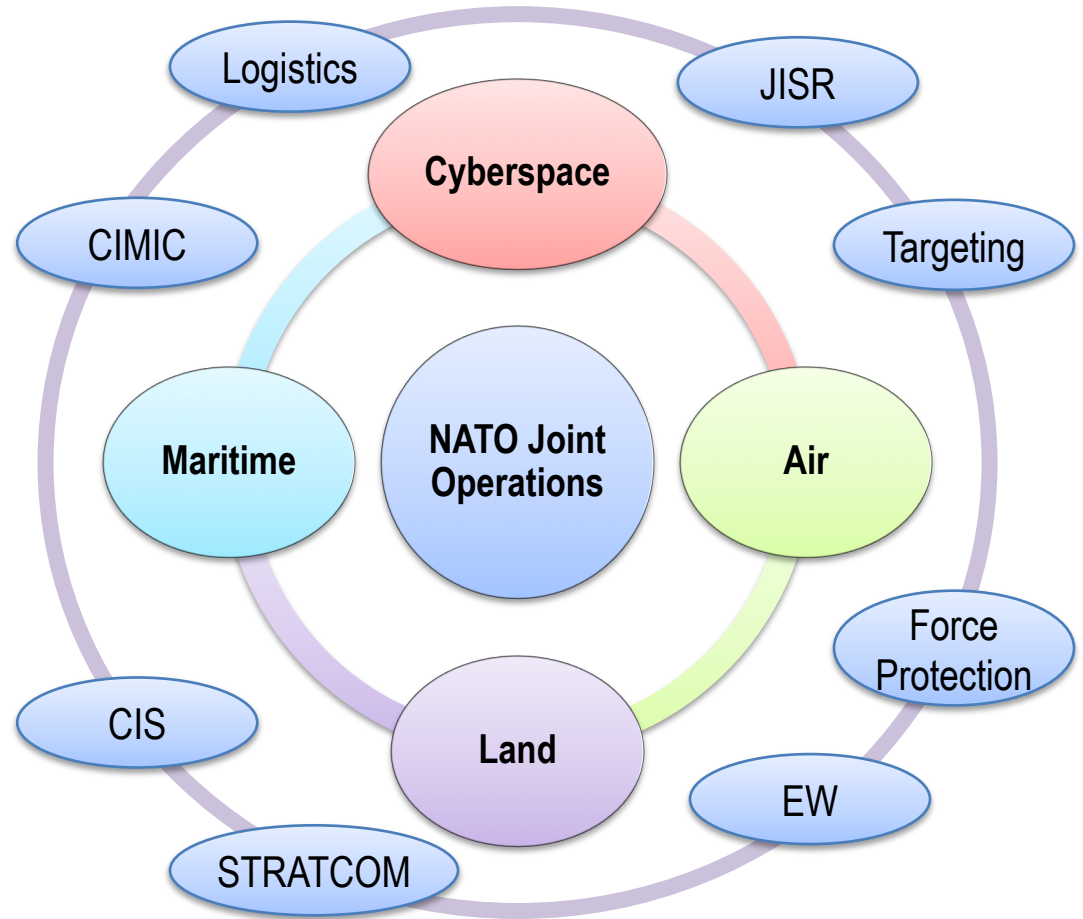
Integration with Other Operational Domains



1

Integrating
with Joint
Operations

Integration with Supporting Disciplines

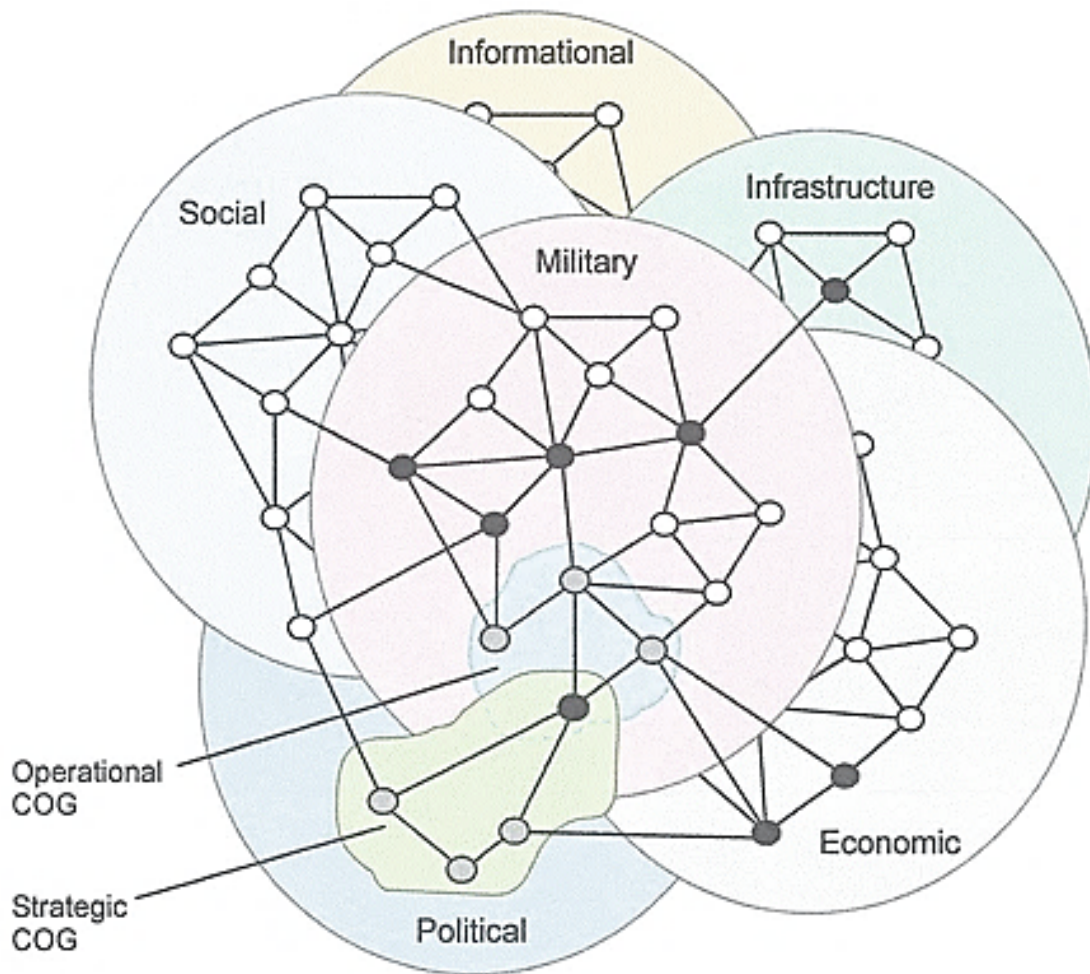


1

Integrating
with Joint
Operations

The Interconnected Operational Environment

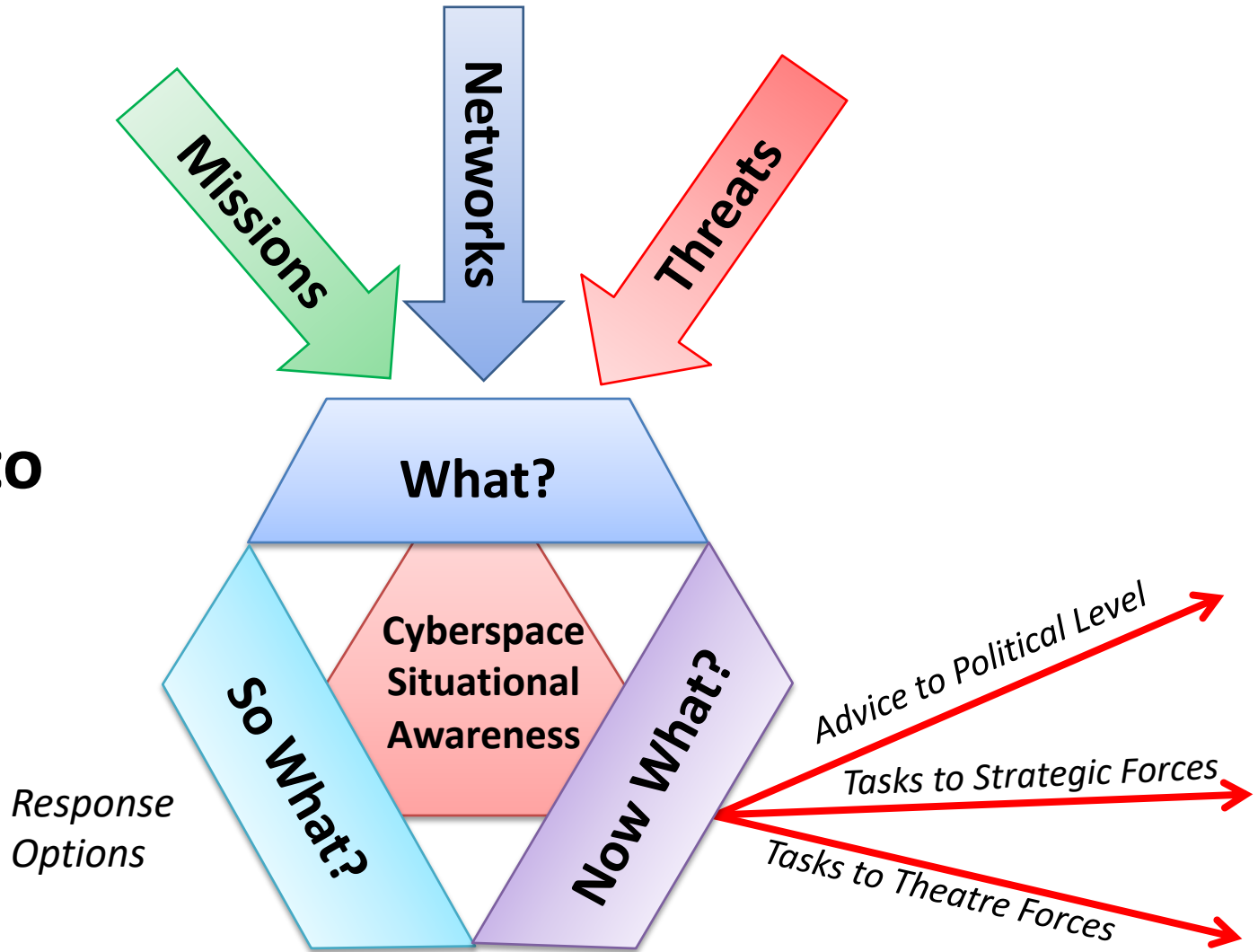
PMESII: Thinking in Systems



1

Integrating
with Joint
Operations

Integrated Approach to Situational Awareness



1

Integrating
with Joint
Operations

Established Operational Planning Process



**Cyberspace as an
Operational Capability**

NATO Crisis Response Process

Indications
and
Warnings

Assess-
ment

Response
Options
Develop-
ment

Planning

Execution

Transition

1

Integrating
with Joint
Operations

Effective Decision-Making Model





Cyberspace Operations Centre

- **Mission:**
 - Provides persistent, centralized and comprehensive cyberspace situational awareness
 - Provide cyberspace domain aspects of mission assurance
 - Focal point for the preparation, planning, conduct and coordination or execution of cyberspace operations

But What About the Unique Aspects?

Cyberspace as an Operational Domain



2

Addressing
Unique
Aspects

Immaturity

**Land Warfare:
5,000+ Years Experience**



2

Addressing
Unique
Aspects

Immaturity

**Sea Warfare:
2,500+ Years Experience**



2

Addressing
Unique
Aspects

Immaturity

**Air Warfare:
100+ Years Experience**



2

Addressing
Unique
Aspects

Immaturity

Cyberspace Warfare?





**CYBERSPACE
IS
ALWAYS
ON**

Threats

- Range from Nation/States to Non-State actors to Individuals
- Able to affect both specific and broad-based targets
- Often operating below the level of Crisis
- Advanced Persistent Threats:
 - Long term preparation of targets
 - Sophisticated effects

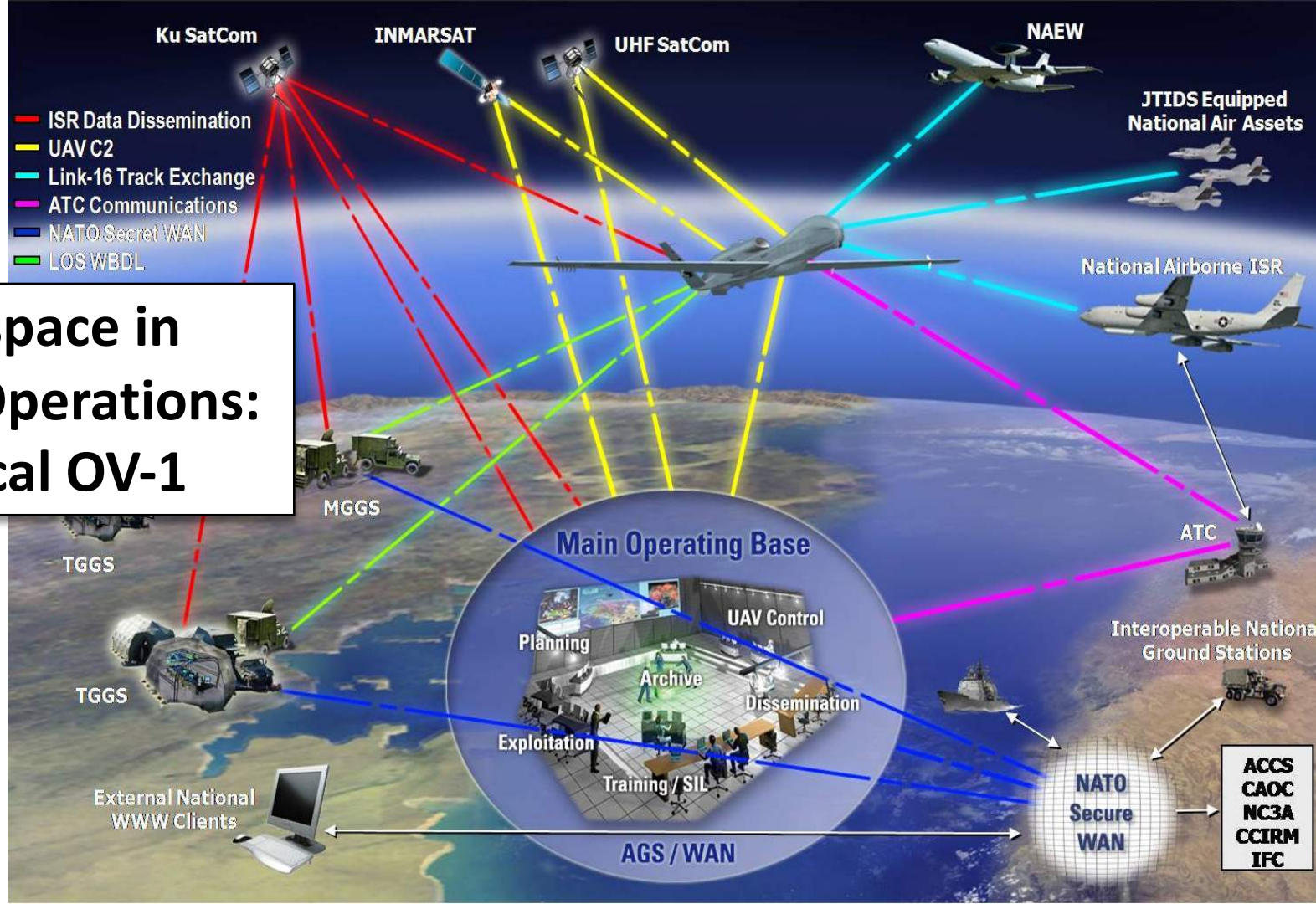
Persistence

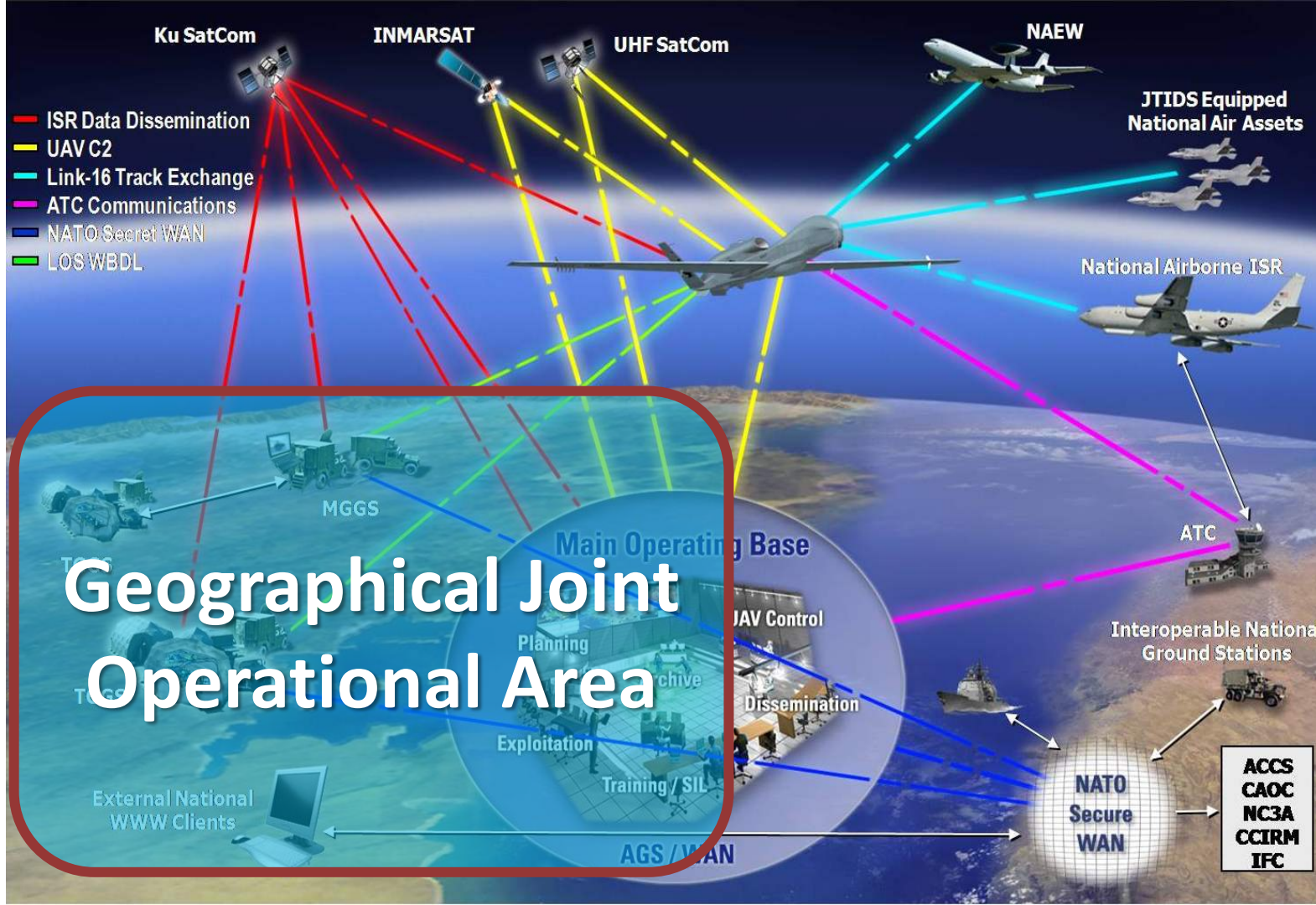


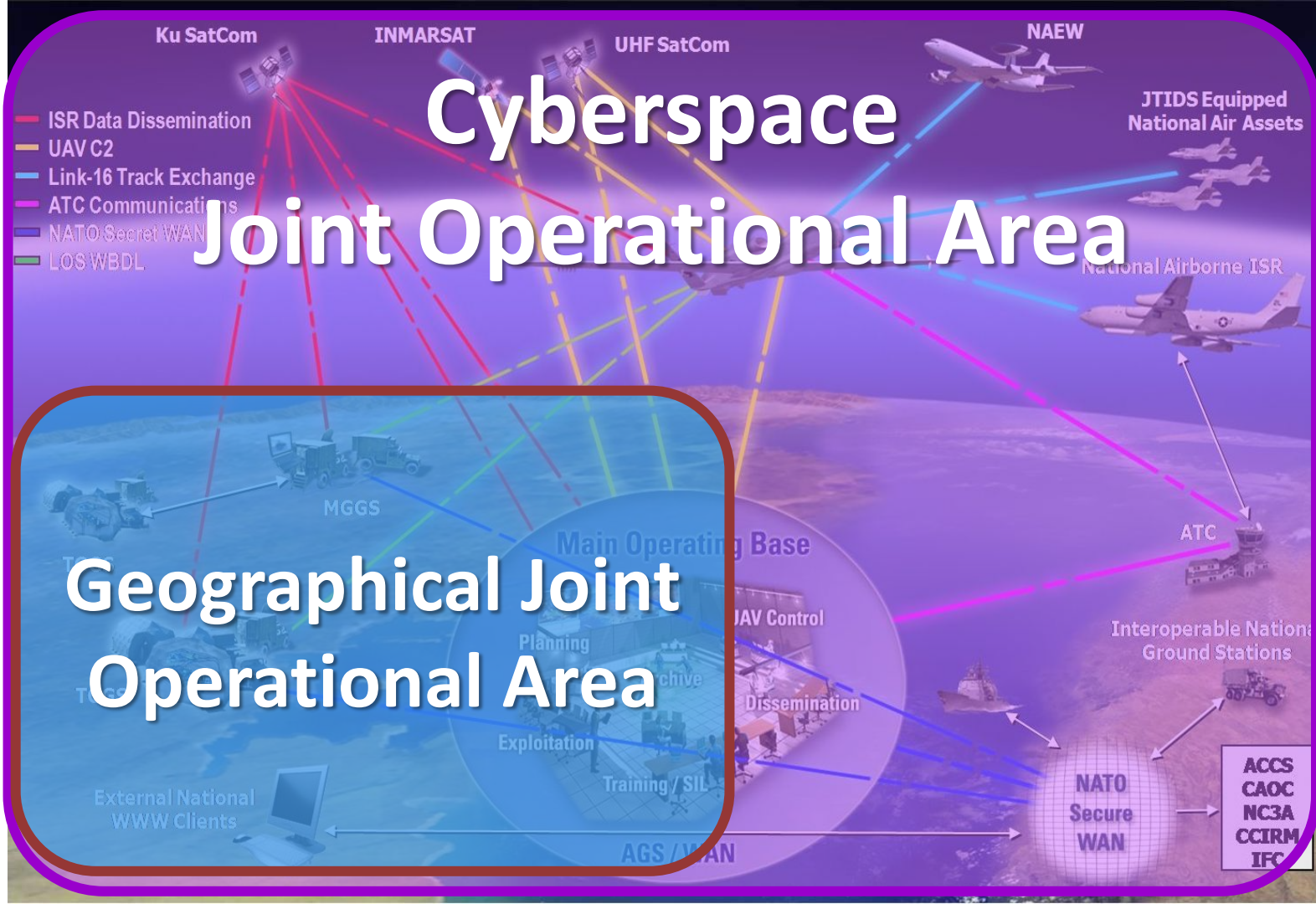
**CYBERSPACE
IS
ALWAYS
ON**

- Cyber Defence has to be a “Day Zero” capability
- Everyday cyber incidents offer opportunities for collaboration and learning
- Effective NATO-National coordination requires regular practice through exercises and training

Cyberspace in Military Operations: A Typical OV-1







Cyberspace Area of Interest

**Law
Enforcement**

**Civil &
Commercial
Spectrum**

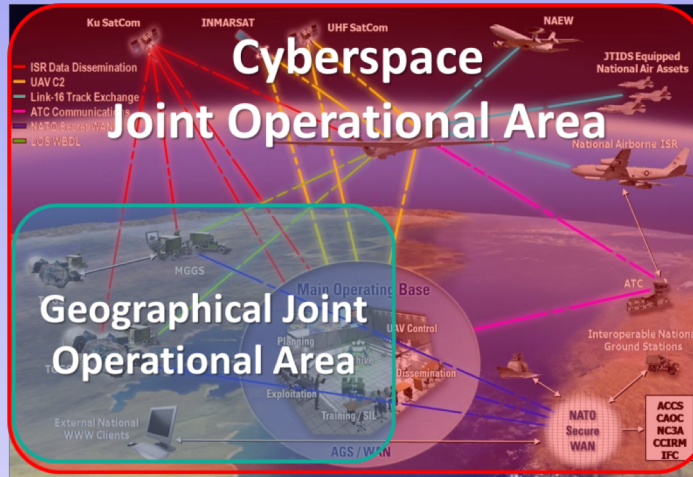
Social Media

NGOs

**Civil
Government
IT**

**Commercial
Providers**

**Critical
National
Infrastructures**



Cyberspace Area of Interest

Law
Enforcement

Civil
Government
IT

Civil &
Commercial

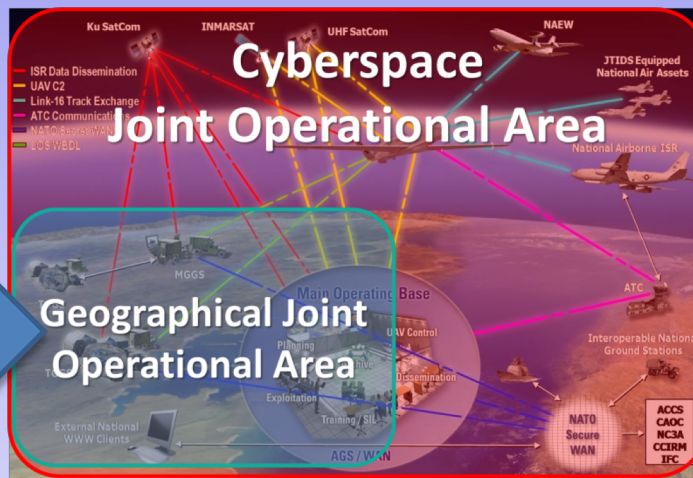
*Within the Theatre Commander's
Control and Means to Affect*

Commercial
Providers

Social Media

NGOs

Critical
National
Infrastructures



Cyberspace Area of Interest

Law
Enforcement

Civil
Government
IT

*Within a Strategic Cyber Commander's
Control and Means to Affect*

Civil &
Commercial

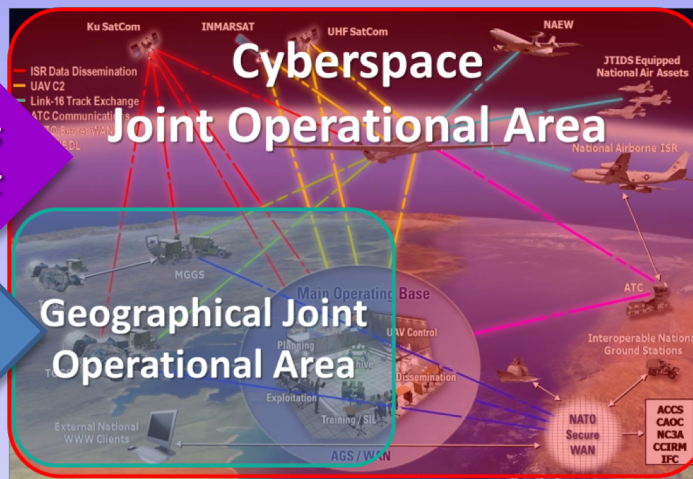
*Within the JTF Commander's Control
and Means to Affect*

Commercial
Providers

Social Media

NGOs

Critical
National
Infrastructures



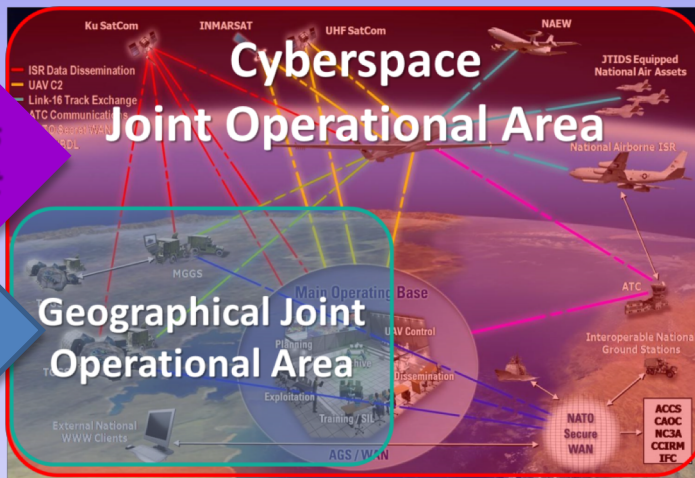
2

Cyberspace Area of Interest

*Outside of Military Control
(and Means to Affect?)*

*Within a Strategic Cyber Commander's
Control and Means to Affect*

*Within the JTF Commander's Control
and Means to Affect*



Civil
Government
IT

Commercial
Providers

Critical
National
Infrastructures

Social Media

NGOs

2

Addressing
Unique
Aspects

Hackers Incoming!

**Some Analogies
Don't Work**

**Whether for
Defense . . .**



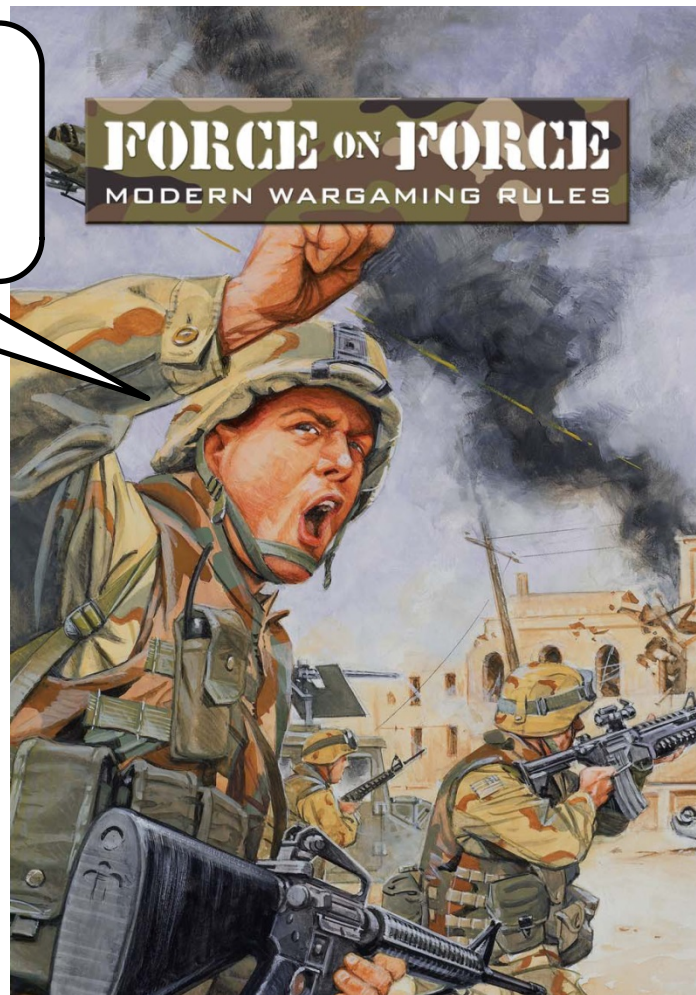
2

Addressing
Unique
Aspects

*Let's Take Out Those
@%*& Hackers!*

**Some Analogies
Don't Work**

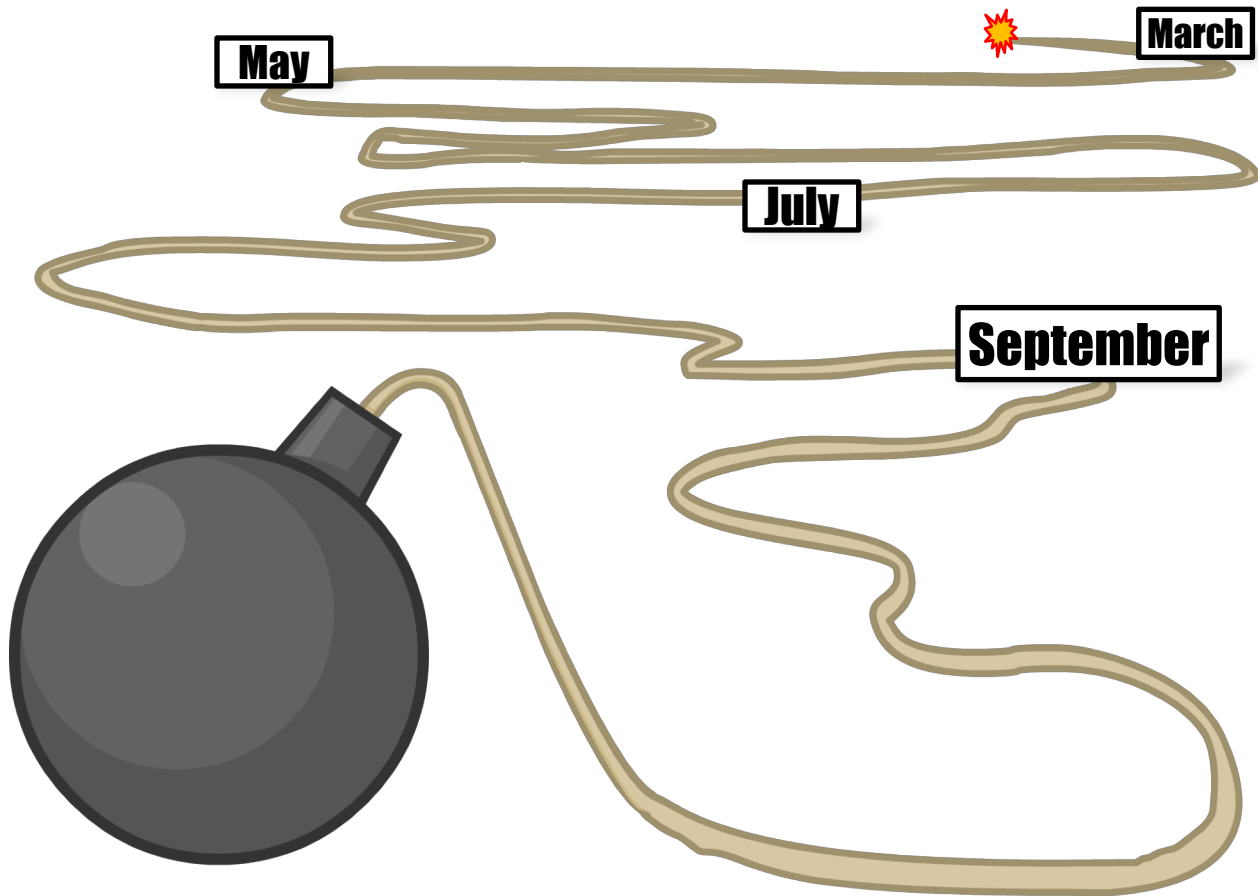
... Or for Offense



2

Addressing
Unique
Aspects

**Cyber Attacks
Can Take a
Long Time to
Take Effect**



2

Addressing
Unique
Aspects

**... Or Not
Even Be
Noticed**



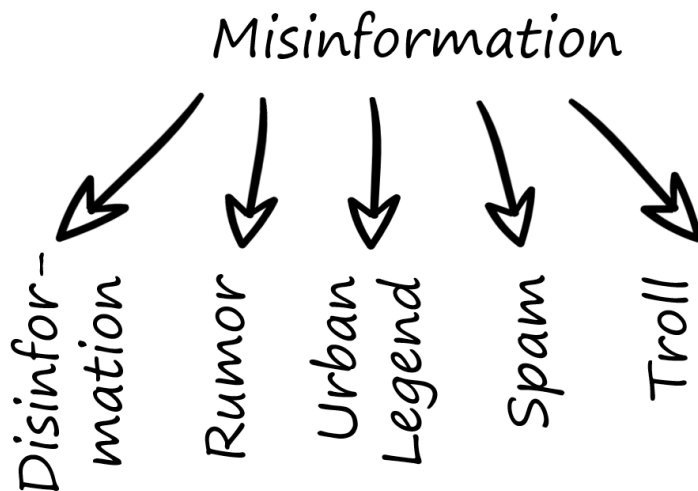
Cyberspace Defence is About Getting Smart About Disinformation

The Russian propaganda guide to stealing your roommate's burrito

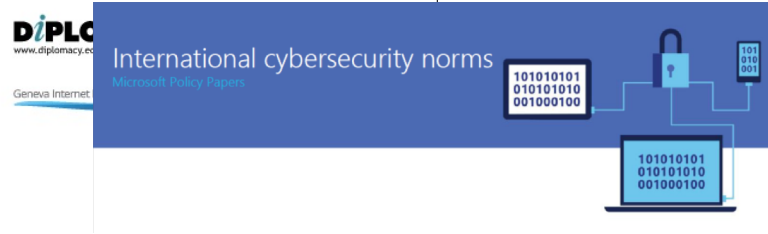
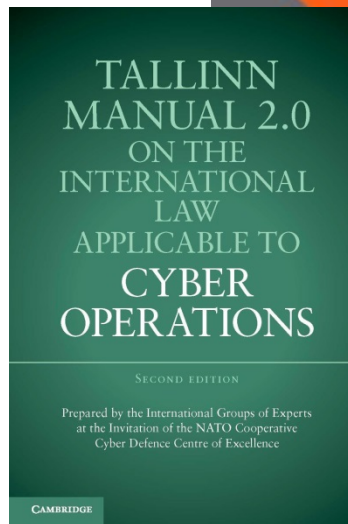
By Natalia Antonova Posted in [Commentary](#) [Crime](#) [Humor](#)

Posted on June 7, 2018

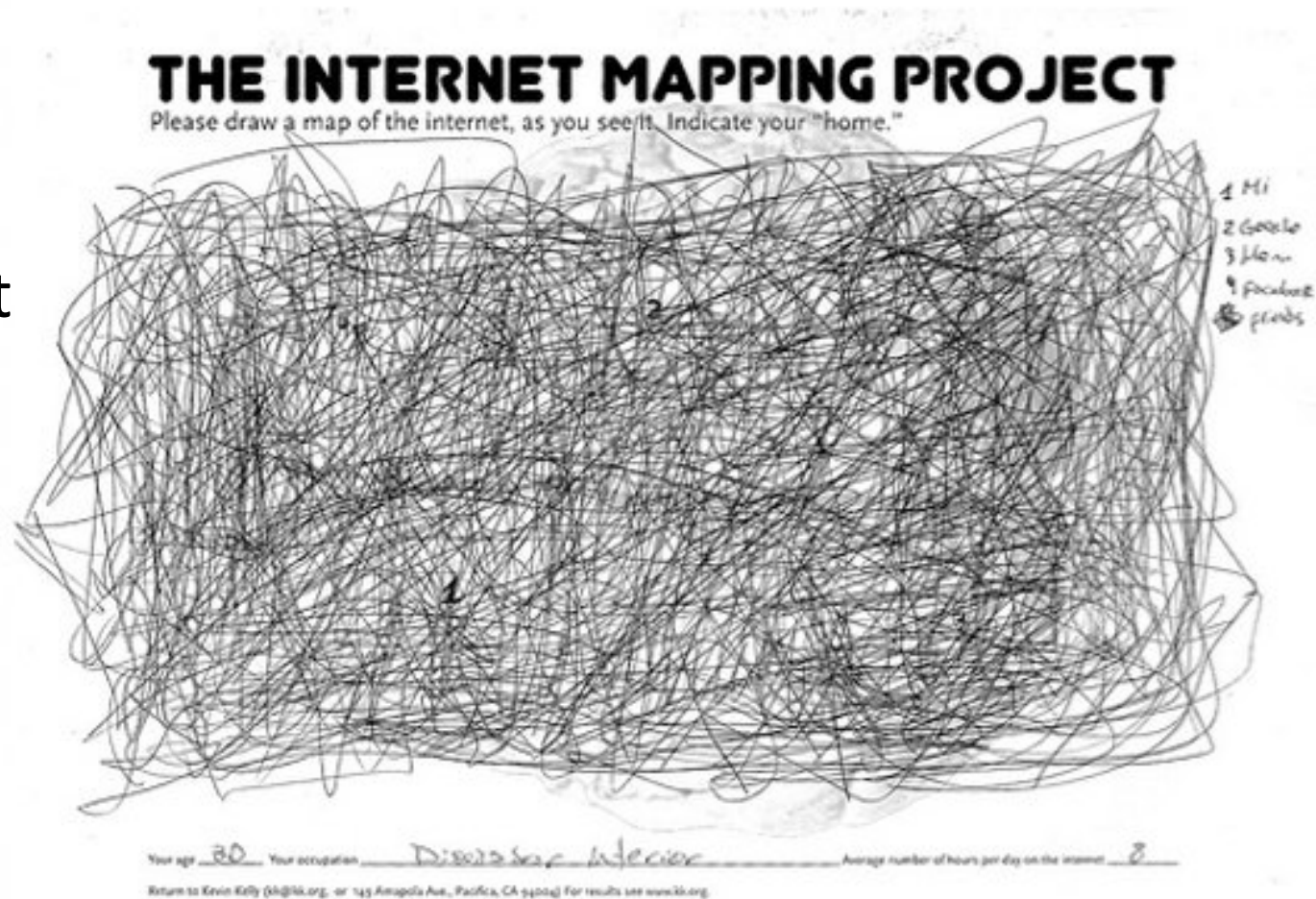
New Study Finds Fake News Spreads Faster and Deeper Than Verified Stories on Twitter



Cyberspace Defence is About Establishing Norms of Behavior

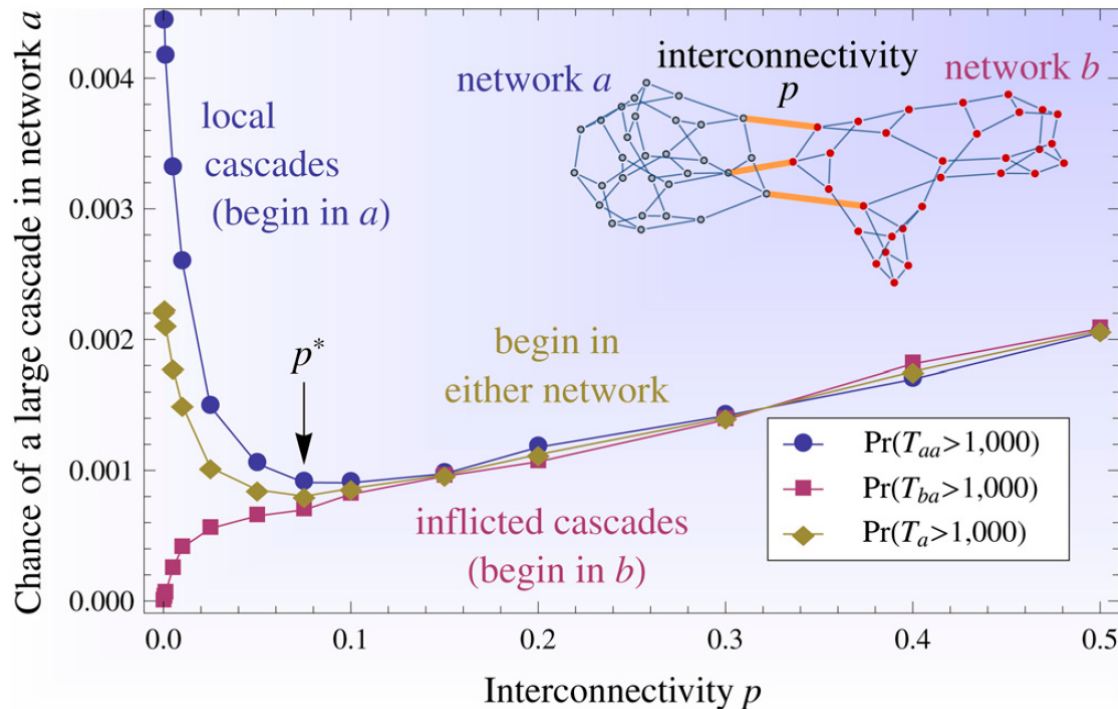


Cyberspace isn't
one Network:
It's a Network
of Networks
of Networks



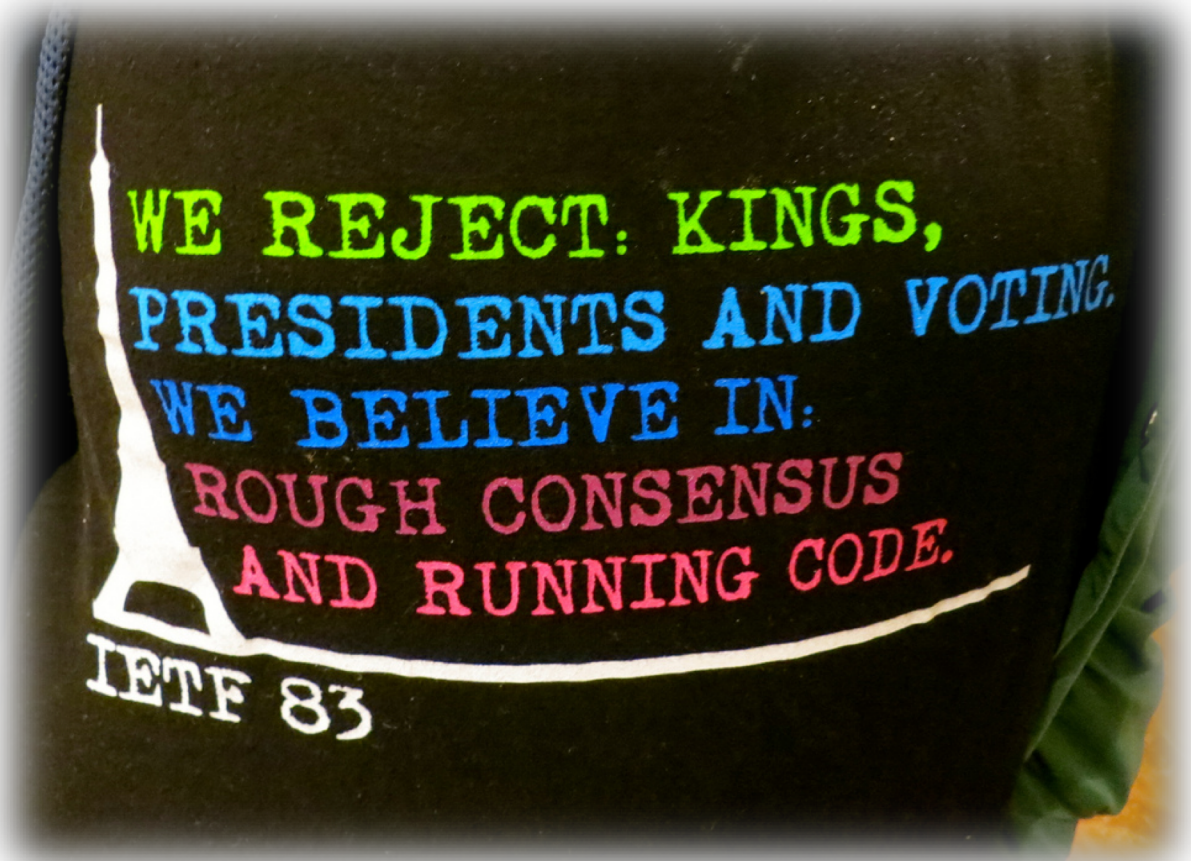
Cyberspace isn't one Network: It's a Network of Networks of Networks

... which can result in
complex, Nth order effects



Source: Suppressing cascades in interdependent networks
Charles D. Brummitta, Raissa M. D'Souza and E. A. Leicht
www.pnas.org/cgi/doi/10.1073/pnas.1110586109

Much of Cyberspace Is Governed Through Rough Consensus



Cyberspace Defence is Decentralized



Is Cyber War a Reality?

1. What Happens in Cyberspace Affects How We Would Fight a War

2. How We Defend Cyberspace is About Much, Much More than Just the Military's Role



**Cyber Defence
is a Team Sport**