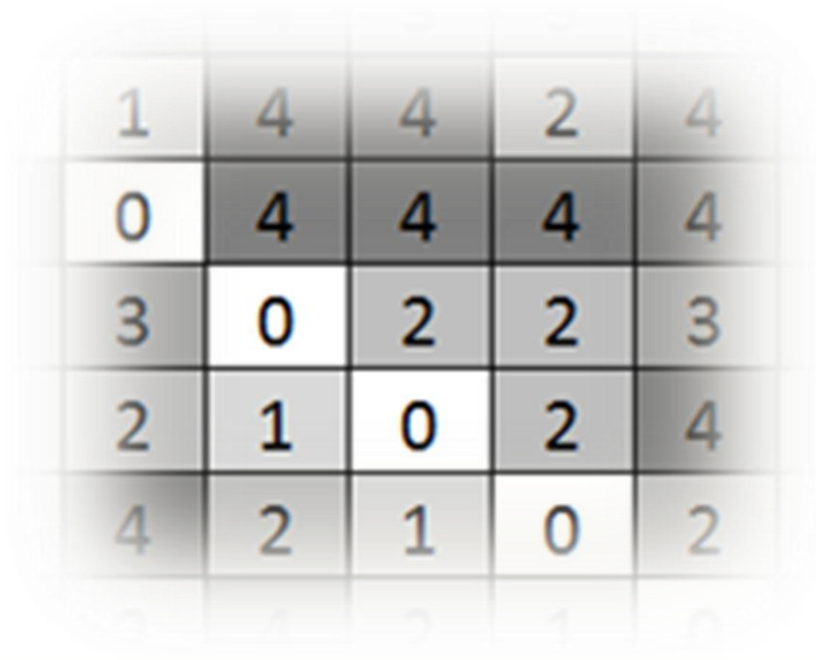


1	4	4	2	4
0	4	4	4	4
3	0	2	2	3
2	1	0	2	4
4	2	1	0	2

Nation-State Cyber Attack Mitigation Strategies: DEMATEL Analysis

Kenneth Geers

NCIS / CCD CoE

These views do not represent official USG, NATO or CCD CoE positions.

About me

- 2007-2011: Scientist, U.S. Representative (1st)
  - NATO Cyber Centre of Excellence, Estonia
- 2001-2007: Division Chief for Cyber Analysis (2nd)
  - Naval Criminal Investigative Service (NCIS), USA
- 1999–2001: Web/VB Dev, Security Studies (1st)
  - Science Applications International Corp, USA
- 1993–2002: Signals Intelligence Analyst
  - U.S. Army Reserve, National Security Agency

National Security Perspective

- All conflicts now have cyber dimension
  - Espionage, propaganda, DoS, infrastructure
  - Cyber terror / cyber war ?
- Strategic problems req strategic solutions
  - Nation-state, international
  - Beyond tactical, temporary fixes
  - Many unanswered questions!

Research Question

* How to prioritize nation-state cyber attack mitigation strategies?

1. Next-Generation Internet: IPv6
2. Sun Tzu’s *Art of War*
3. Cyber attack deterrence
4. Cyber arms control

Research Outline 1

1. Cyber security
   - Technical discipline to strategic concept
2. Technical primer
   - Hacking, security analysis, simulations
3. Real-world impact
   - Internal security, international conflict, case studies

Research Outline 2

4. Threat mitigation strategies
   – Technical, military, political
5. DEMATEL method
   – Aid to strategic analysis
   – Calculation of indirect influence
6. Strategy prioritization
   – Recommendation to policymakers

Mitigation Strategy Categories

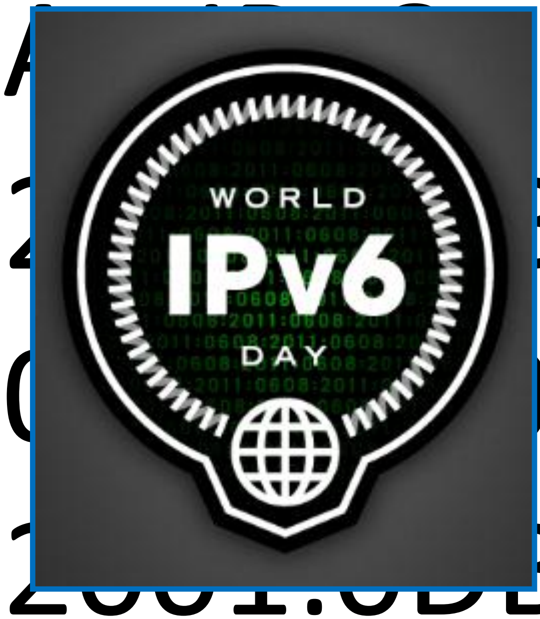
1. IPv6 → Technical
2. *Art of War* → Military
3. Deterrence → Military / Political
4. Arms control → Political / Technical

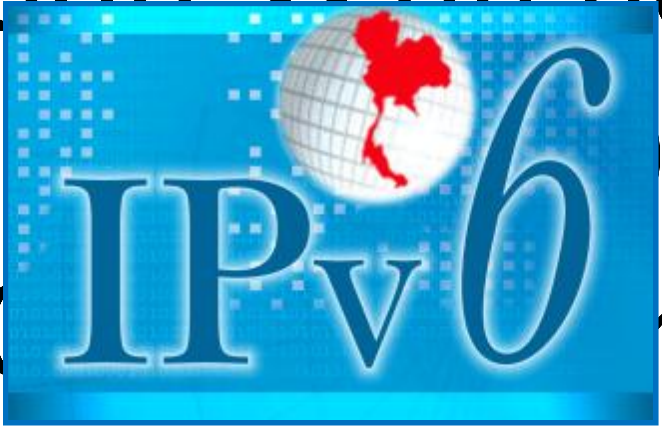
A ddress (in hexadecimal)

2 3 1 0

0 0 n e

2001:0DB8:AC10:FE01:: 0





0 0001101101111000:

0 0 0

0 0 0

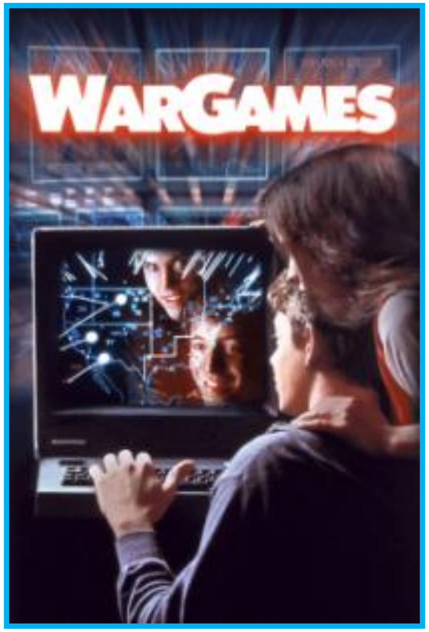
0 :0 0

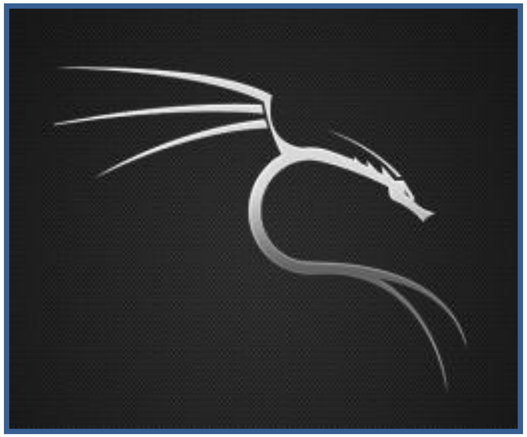
0000000000000000 0000000000

Internet Protocol version 6 (IPv6)

- Reduces anonymity
  - China: “Everyone” US: “Everything”
  - Limitless IPs, NAT not required
- Security game-changer
  - Native IPSec: authentication, encryption
- No silver bullet
  - SW/users still vulnerable
  - Privacy, politics, learning curve

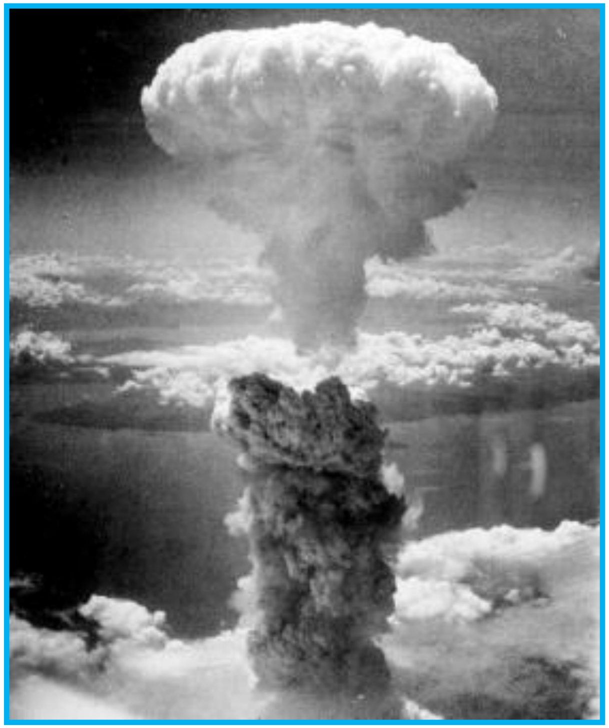
孫子兵法

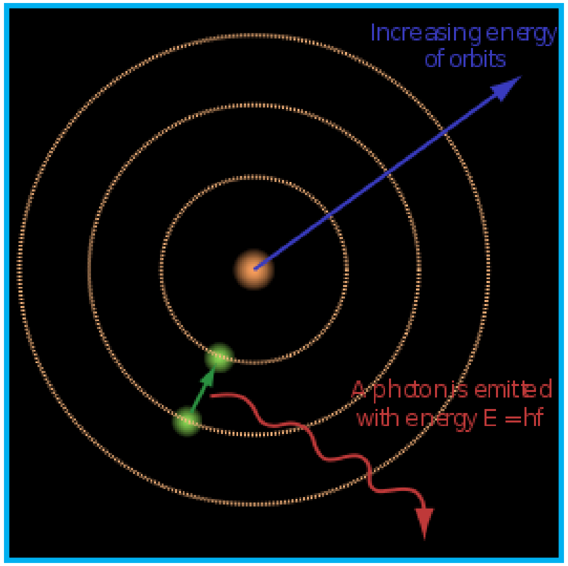




Sun Tzu's *Art of War*

- Good … not perfect guide to cyber conflict
- *Art of Cyber War*
  1. Artificial environment
  2. Geography changes without warning
  3. Physical proximity loses relevance
  4. Blinding development of technology
  5. Anonymity
  6. Few moral inhibitions





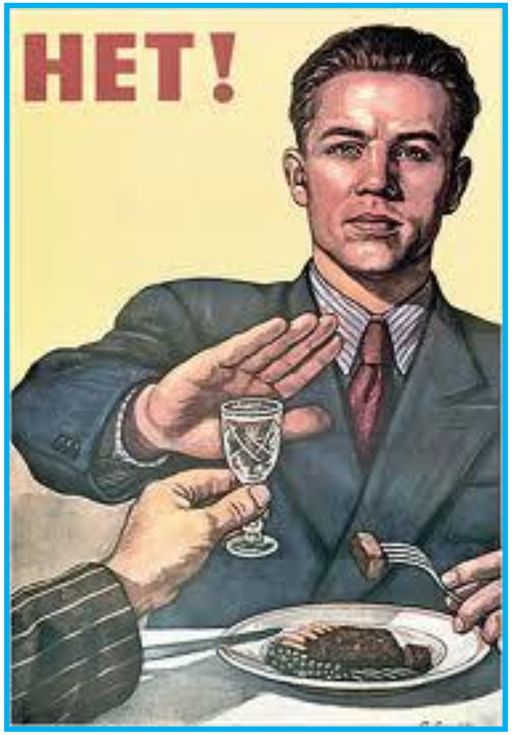
Increasing energy
of orbits
A photon is emitted
with energy E = hf

Cyber Attack Deterrence

- Deterrence options
  1. Denial
  2. Punishment
- Deterrence requirements
  1. Capability
  2. Communication
  3. Credibility
- Mutually Assured Disruption?

UN

The highest capacity
Flash drive on the market
DT310


НЕТ!

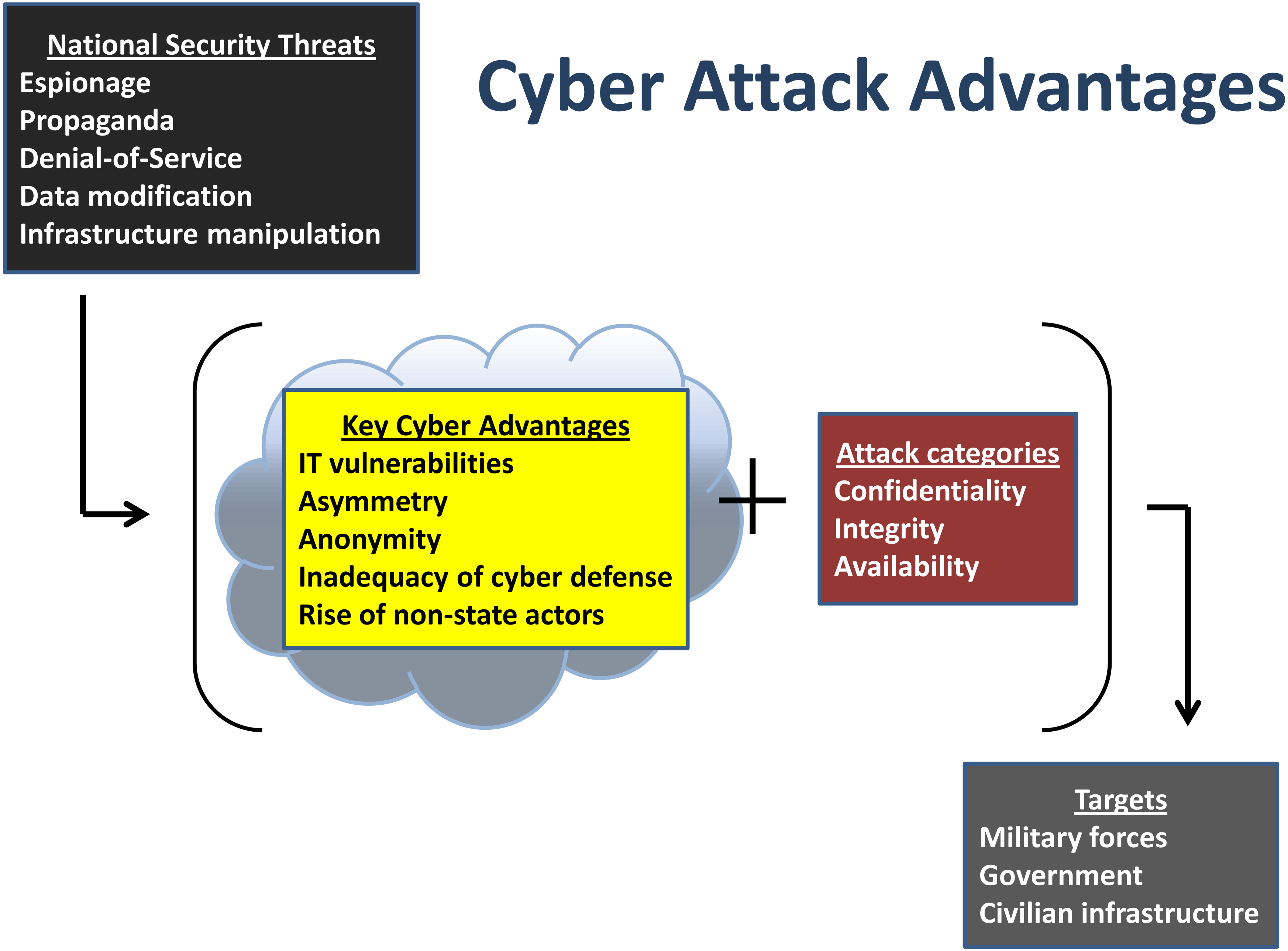
Cyber Arms Control

- Model: Chemical Weapons Convention
  - *Cyber Weapons Convention*?
- Easy to apply
  1. Political will
  2. Universality
  3. Assistance
- Hard to apply
  4. Prohibition
  5. Inspection

DEMATEL: “Influencing Factors”

National Security Threats	Cyber Attack Advantages	Attack Categories	Targets	Mitigation Strategies	Effectiveness
Espionage	Myriad IT vulnerabilities	Confidentiality	Military forces	IPv6	Solves some Q’s, creates others
Propaganda	Asymmetry	Integrity	Gov/Civ infrastructure	Sun Tzu	Cyber war has unique aspects
Denial-of-Service	Anonymity	Availability		Deterrence	Lacks credibility
Data modification	Inadequacy of cyber defense			Arms Control	Hard to prohibit, inspect cyber
Infrastructure manipulation	Rise of non-state actors				

Cyber Attack Advantages



National Security Threats

Espionage
Propaganda
Denial-of-Service
Data modification
Infrastructure manipulation

Key Cyber Advantages

IT vulnerabilities
Asymmetry
Anonymity
Inadequacy of cyber defense
Rise of non-state actors

+

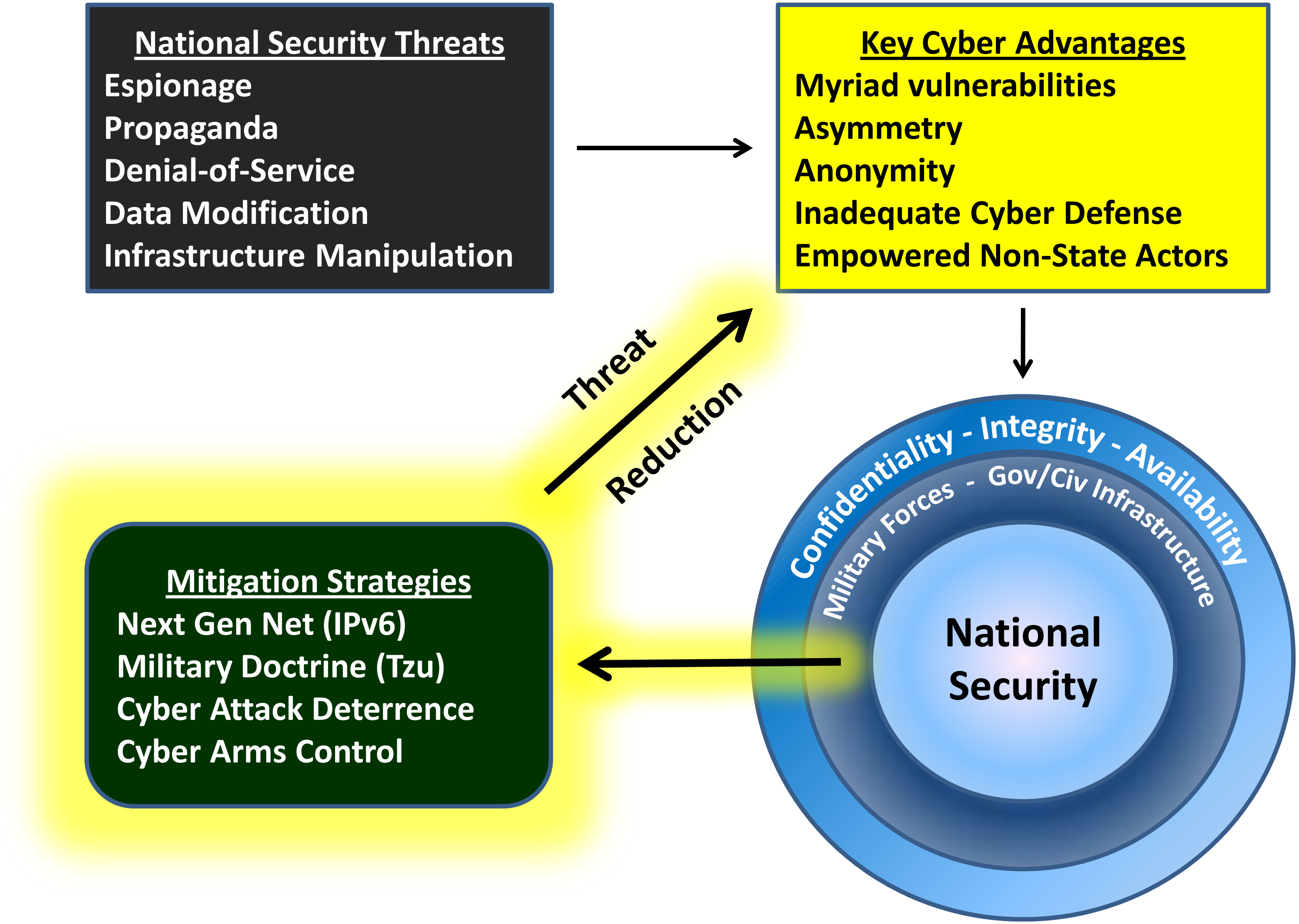
Attack categories

Confidentiality
Integrity
Availability

Targets

Military forces
Government
Civilian infrastructure

Mitigation Strategies



National Security Threats

Espionage
Propaganda
Denial-of-Service
Data Modification
Infrastructure Manipulation

Key Cyber Advantages

Myriad vulnerabilities
Asymmetry
Anonymity
Inadequate Cyber Defense
Empowered Non-State Actors

Mitigation Strategies

Next Gen Net (IPv6)
Military Doctrine (Tzu)
Cyber Attack Deterrence
Cyber Arms Control

Threat
Reduction
Confidentiality - Integrity - Availability
Military Forces - Gov/Civ Infrastructure
National Security

Strategy Review

Strategy	Evaluation
IPv6	Increases attribution by lowering anonymity IPsec authenticates, encrypts; not mandatory Long, dangerous transition phase
Art of War	Sun Tzu good but not perfect Concepts, law behind tech curve Cyber warfare has distinctive characteristics
Deterrence	Denial difficult, hacker skills easy to acquire Punishment lacks credibility Low attribution, high asymmetry, no one dies
Arms Control	How to prohibit what is hard to define? How to inspect cyberspace? Political will could change dynamics

All could help …

But each is only a partial solution

DEMATEL Influence Matrix *X*

	DEMATEL "Expert Knowledge" Influence Matrix *X* None = 0 Low = 1 Medium = 2 High = 3 Very high = 4	A	B	C	D	E	F	G	H	I	
		IT vulnerabilities	Asymmetry	Anonymity	Inadequate cyber defense	Empowered non-state actors	Next Gen Internet: IPv6	Best mil doctrine: Sun Tzu	Cyber attack deterrence	Cyber arms control	Direct Influence
A	IT vulnerabilities	0	4	4	4	3	3	2	3	3	26
B	Asymmetry	2	0	1	4	4	2	4	4	3	24
C	Anonymity	2	4	0	4	4	4	4	4	4	30
D	Inadequate cyber defense	4	3	3	0	2	2	3	4	2	23
E	Empowered non-state actors	1	2	2	1	0	2	4	3	3	18
F	Next Gen Internet: IPv6	3	2	4	2	1	0	2	2	2	18
G	Best mil doctrine: Sun Tzu	3	3	2	4	2	1	0	4	2	21
H	Cyber attack deterrence	1	2	2	2	2	1	2	0	3	15
I	Cyber arms control	1	1	2	2	2	1	2	3	0	14
	Level Influenced	17	21	20	23	20	16	23	27	22	

“Direct Influence” by Factor

Factor		Direct Influence
C	Anonymity	30
A	IT vulnerabilities	26
B	Asymmetry	24
D	Inadequate cyber defence	23
G	Best mil doctrine: Sun Tzu	21
E	Empowered non-state actors	18
F	Next Gen Internet: IPv6	18
H	Cyber attack deterrence	15
I	Cyber arms control	14

↑ Reality ↓

↑ Ideas ↓

Susceptibility to Influence

Factor		Susceptibility to Influence
H	Cyber attack deterrence	27
G	Best mil doctrine: Sun Tzu	23
D	Inadequate cyber defence	23
I	Cyber arms control	22
B	Asymmetry	21
E	Empowered non-state actors	20
C	Anonymity	20
A	IT vulnerabilities	17
F	Next Gen Internet: IPv6	16

↑

Less Reliable

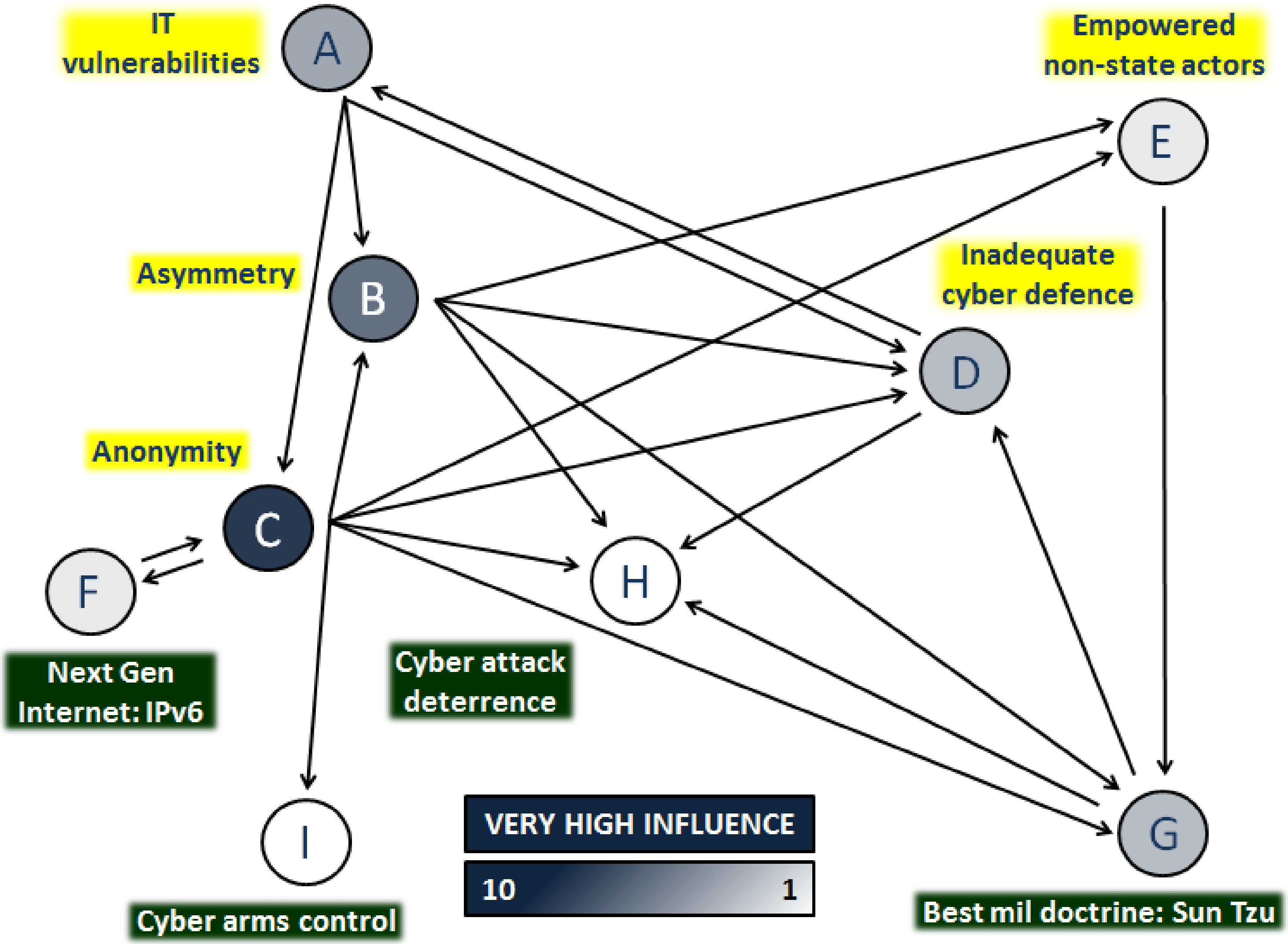
↓

↑

More Reliable

↓

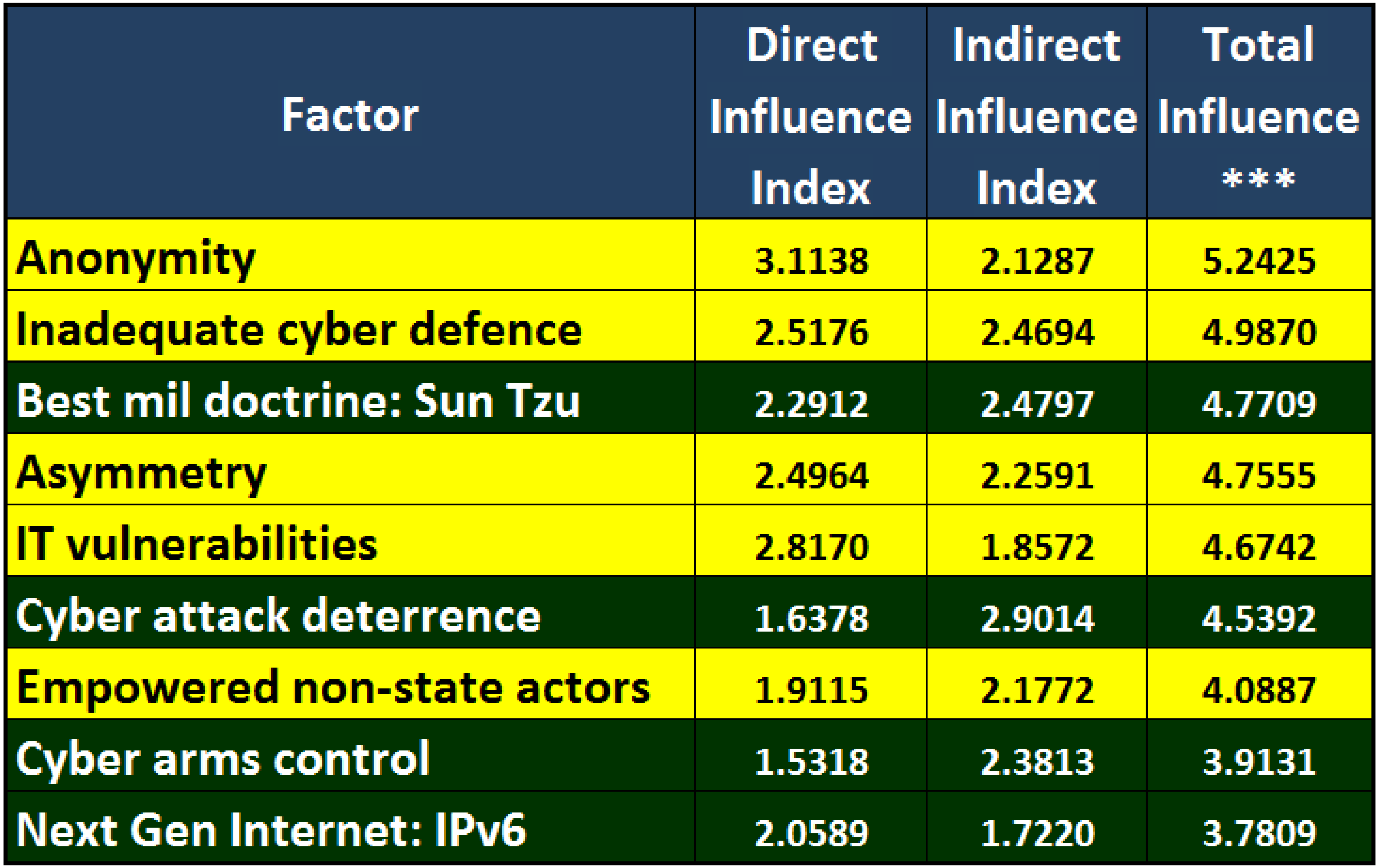
Causal Loop Diagram



“Total Influence” Matrix *T*

		A	B	C	D	E	F	G	H	I	
	DEMATEL “Total Influence” Matrix *T*	IT vulns	Asymmetry	Anonymity	Inad cyb def	Non-state act	Next Gen Net	Best mil doc	Deterrence	Arms control	Direct Influence
A	IT vulns	.1850	.3441	.3298	.3645	.3095	.2643	.3114	.3799	.3285	2.8170
B	Asymmetry	.2257	.1954	.2186	.3324	.3075	.2077	.3365	.3747	.2979	2.4964
C	Anonymity	.2664	.3632	.2310	.3867	.3556	.3047	.3911	.4366	.3785	3.1138
D	Inad cyb def	.2842	.2944	.2801	.2223	.2579	.2162	.3101	.3771	.2753	2.5176
E	Non-state act	.1562	.2117	.2022	.1997	.1448	.1738	.2856	.2867	.2508	1.9115
F	Next Gen Net	.2274	.2305	.2765	.2462	.1947	.1295	.2427	.2740	.2374	2.0589
G	Best mil doc	.2420	.2749	.2329	.3201	.2397	.1712	.1999	.3555	.2550	2.2912
H	Deterrence	.1386	.1906	.1821	.2038	.1884	.1304	.2063	.1687	.2289	1.6378
I	Arms control	.1317	.1543	.1755	.1937	.1791	.1242	.1961	.2482	.1290	1.5318
	Indirect Influence	1.8572	2.2591	2.1287	2.4694	2.1772	1.7220	2.4797	2.9014	2.3813	

Combined Influence Index



Factor	Direct Influence Index	Indirect Influence Index	Total Influence ***
Anonymity	3.1138	2.1287	5.2425
Inadequate cyber defence	2.5176	2.4694	4.9870
Best mil doctrine: Sun Tzu	2.2912	2.4797	4.7709
Asymmetry	2.4964	2.2591	4.7555
IT vulnerabilities	2.8170	1.8572	4.6742
Cyber attack deterrence	1.6378	2.9014	4.5392
Empowered non-state actors	1.9115	2.1772	4.0887
Cyber arms control	1.5318	2.3813	3.9131
Next Gen Internet: IPv6	2.0589	1.7220	3.7809

Final Index

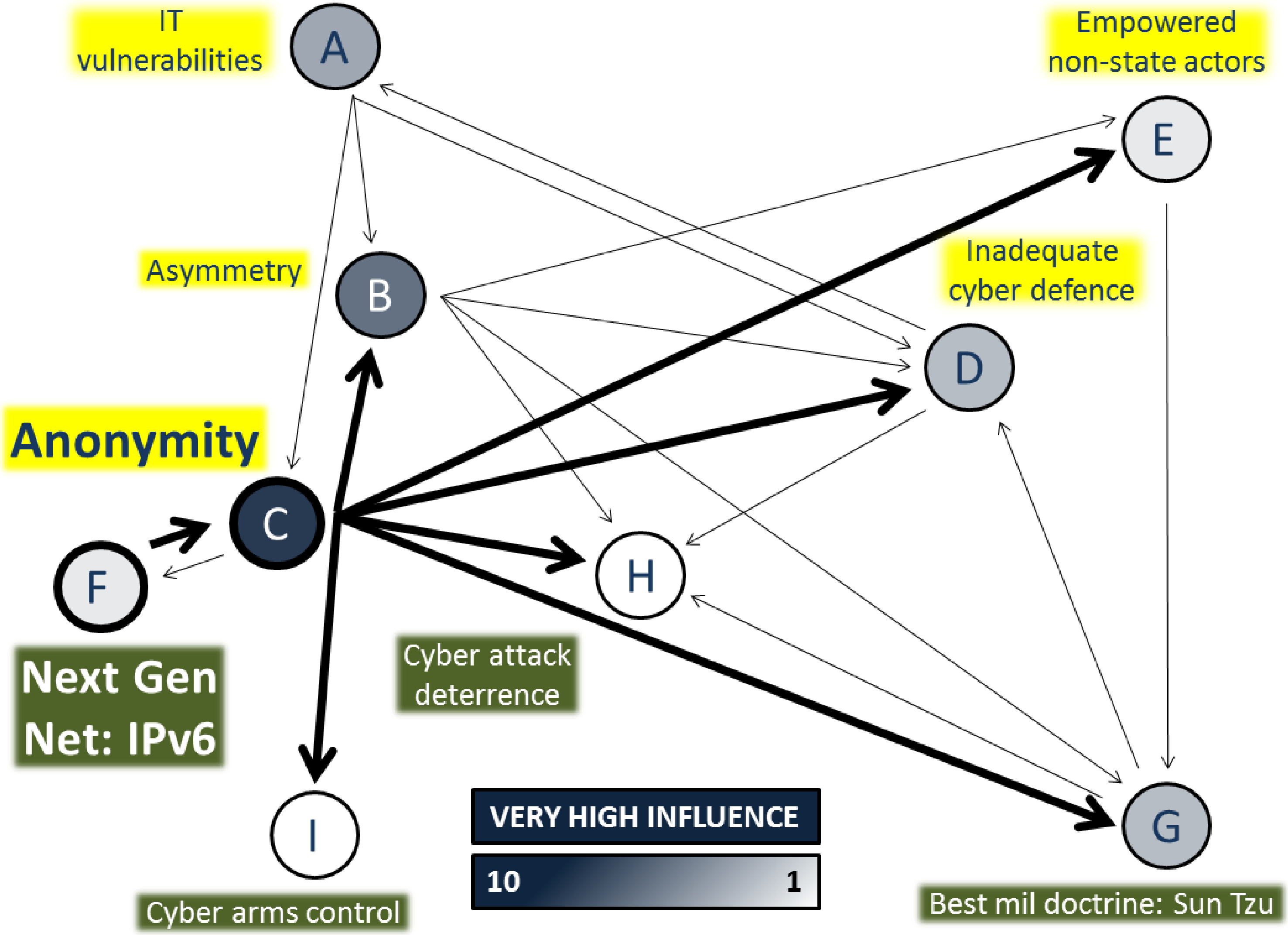
	DEMATEL Normalized “Total Influence” Index	Score
1	Anonymity	.9851
2	IT vulnerabilities	.9598
3	Next Gen Internet: IPv6	.3369
4	Asymmetry	.2373
5	Inadequate cyber defence	.0481
6	Best mil doctrine: Sun Tzu	-.1886
7	Empowered non-state actors	-.2654
8	Cyber arms control	-.8496
9	Cyber attack deterrence	-1.2636

Indirect Influence Impact

Anonymity	30
IT vulnerabilities	26
Asymmetry	24
Inad cyber def	23
Doctrine: Sun Tzu	21
Non-state actors	18
Next Gen Net: IPv6	18
Deterrence	15
Cyber arms control	14

Anonymity	.9851
IT vulnerabilities	.9598
Next Gen Net: IPv6	.3369
Asymmetry	.2373
Inad cyber def	.0481
Doctrine: Sun Tzu	-.1886
Non-state actors	-.2654
Cyber arms control	-.8496
Deterrence	-1.2636

IPv6 System Impact



Cyber Attack Advantages

Before:		**After:**
1. Anonymity	→	1. Anonymity
2. Vuln IT Infrastr	→	2. Vuln IT Infrastr
3. Asymmetry	→	3. Asymmetry
4. Inad cyber def	→	4. Inad cyber def
5. Non-state actors	→	5. Non-state actors

Attack Mitigation Strategies

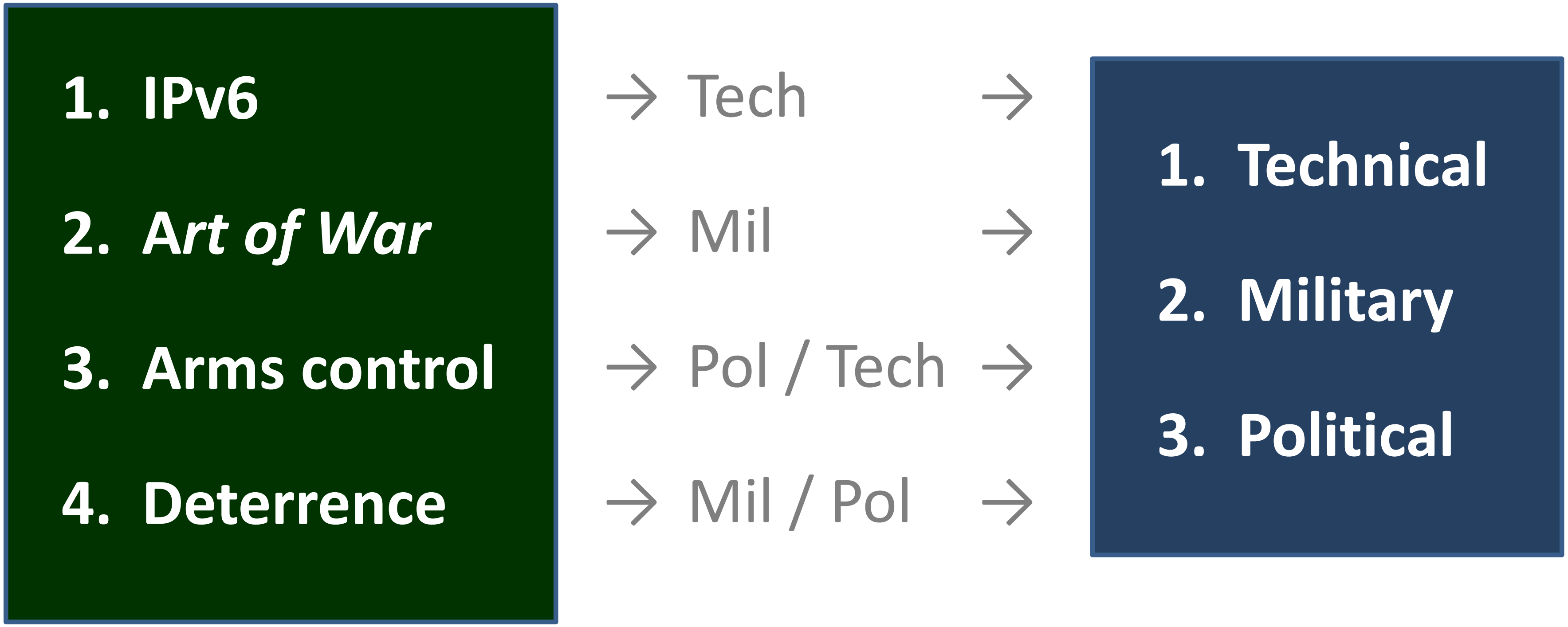
Before:

1. Doctrine: Sun Tzu
2. Next Gen Net: IPv6
3. Deterrence
4. Arms control

After:

1. Next Gen Net: IPv6
2. Doctrine: Sun Tzu
3. Arms control
4. Deterrence

Thesis Conclusion



1. IPv6 → Tech →
2. *Art of War* → Mil →
3. Arms control → Pol / Tech →
4. Deterrence → Mil / Pol →

1. Technical
2. Military
3. Political

Future Work

1. Survey of cyber defense experts
    - Deepen understanding of concepts
2. DEMATEL: individual factors
    - Disaggregate Matrix ***X***
3. DEMATEL: other cyber security challenges
    - Can a cyber attack be an act of war?
    - Can we solve the attribution problem?
    - Can we shift the advantage to cyber defense?

Publications: Thomson Reuters ISI Web of Knowledge

- **“Live Fire Exercise: Preparing for Cyber War”**
  - *Journal of Homeland Security and Emergency Management* 7(1) 1-16 (2010)
- **“Cyber Weapons Convention”**
  - *Computer Law and Security Review* 26(5) 547-551 (2010)
- **“The Challenge of Cyber Attack Deterrence”**
  - *Computer Law and Security Review* 26(3) 298-303 (2010)
- **“Virtual Plots, Real Revolution”** coauthored with R. Temmingh
  - *The Virtual Battlefield: Perspectives on Cyber Warfare* Czosseck & Geers (Eds) Cryptology and Information Security Series (3) Amsterdam: IOS Press (2009)
- **“The Cyber Threat to National Critical Infrastructures: Beyond Theory”**
  - *The Information Security Journal: A Global Perspective* 18(1) 1-7 (2009)
- **“IPv6: World Update”** coauthored with A. Eisen
  - ICIW 2007: Proceedings of the 2nd International Conference on Information Warfare and Security (2007)

Other Publications

- **“Nation-State Cyber Attack Mitigation Strategies: DEMATEL Analysis”**
  - Presented to *Information Security* Lomonosov Moscow State University (2011)
- **“Sun Tzu and Cyber War”**
  - Cooperative Cyber Defence Centre of Excellence Feb 9, 1-23 (2011)
- **“Demystifying Cyber Warfare”**
  - Forthcoming in *per Concordiam* 2(1) 1-6 (2011)
- **“From Cambridge to Lisbon: the quest for strategic cyber defense”**
  - In peer-review at *Journal of Homeland Security and Emergency Management* 1-16 (2011)
- **“A Brief Introduction to Cyber Warfare”**
  - *Common Defense Quarterly* Spring 16-17 (2010)
- **“Belarus in the Context of European Cyber Security”**
  - *The Virtual Battlefield: Perspectives on Cyber Warfare*. Authored by F. Pavlyuchenko, translated from Russian to English by K. Geers (2009)
- **“Cyberspace and the Changing Nature of Warfare”**
  - *Hakin9* E-Book 19(3) No. 6, *SC Magazine* (27 AUG 08), Black Hat Japan (2008)
- **“Greetz from Room 101”**
  - DEF CON, Black Hat (2007)