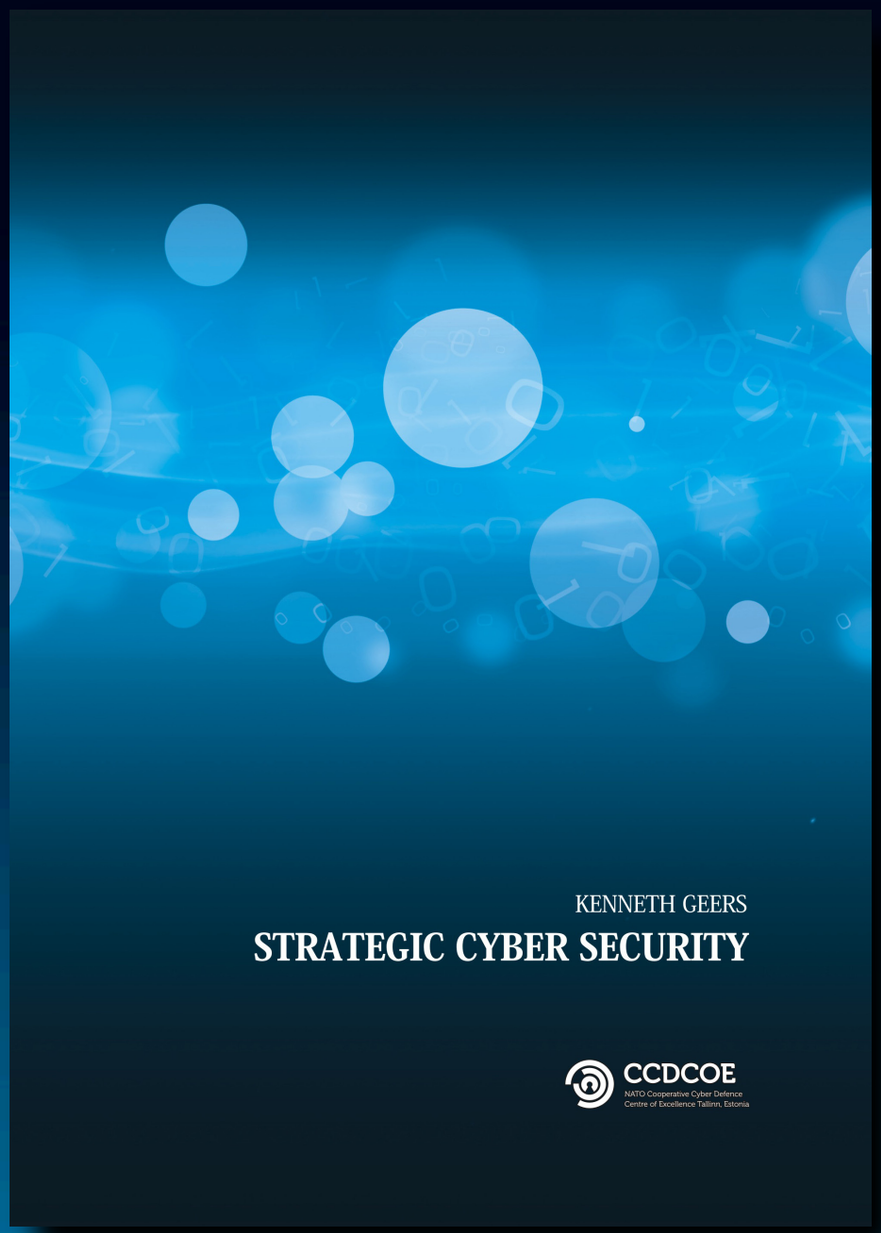


Strategic Cyber Security

An Evaluation of Nation-State Cyber Attack Mitigation Strategies

Kenneth Geers

NCIS Cyber SME

Free download:

ccdcoe.org/278.html

About me

- 2011–: NCIS Cyber Subject Matter Expert
- 2007–2011: NATO Cyber Centre, Estonia
- 2001–2007: NCIS Cyber Analysis (Div Chief)
- 1999–2001: SAIC Security Studies Web/VB Dev
- 1993–2002: USAR SIGINT Analyst, NSA

National Security Perspective

- All conflicts now have a cyber dimension
  - Tactical: espionage, propaganda, DoS, CIP
  - Strategic: terror / war ?
- Strategic problems req strategic solutions
  - Nation-state, international
  - Beyond tactical, temporary fixes

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 I

1. Cyber security

   Technical discipline to strategic concept

2. Technical primer

   Hacking, security analysis, simulations

3. Real-world impact

   Internal security, internat'l conflict, case studies

Research Outline 2

4. Threat mitigation strategies

   Technical, military, political

5. DEMATEL method

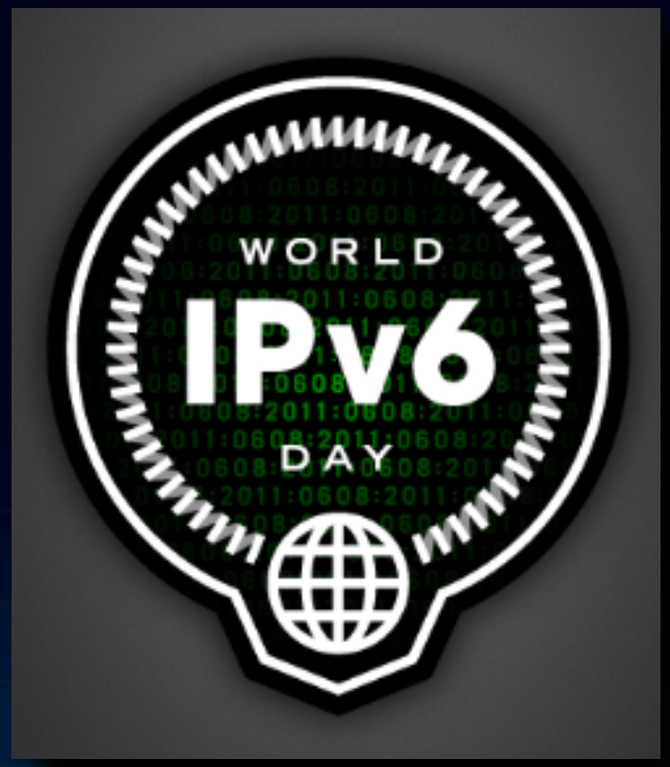
   Strategic analysis / calculate indirect influence

6. Strategy prioritization

   Recommendation to policymakers

Cyber Attack Mitigation Strategies

✳ IPv6	➡ Technical
✳ Art of War	➡ Military
✳ Deterrence	➡ Military / Political
✳ Arms control	➡ Political / Technical







An IPv6 address in hexadecimal 2001:0DB8:AC10:FE01:0000:0000:0000:0000
Zeroes can be omitted: 2001:0DB8:AC10:FE01:: 0010000
000000001:0000110110111000:1010110000010000:1111111100000001:
0000000000000000:00000
00000000000:0000000000000000:0000000000000000:0000000000





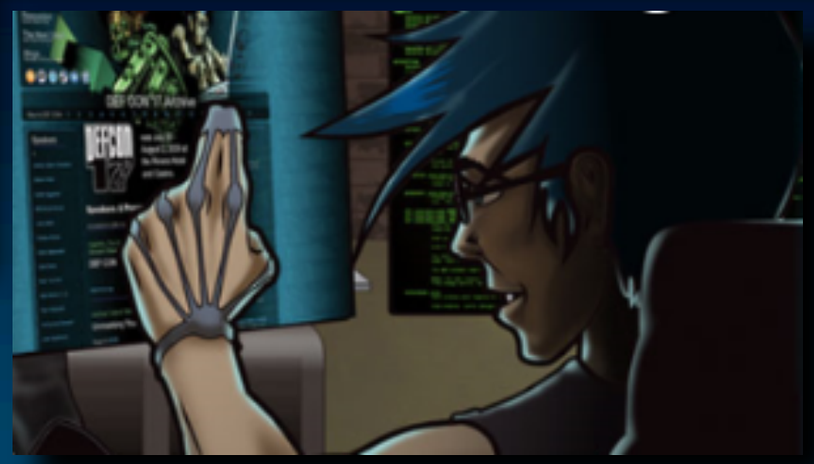
Internet Protocol version 6 (IPv6)

- 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

孫子兵法

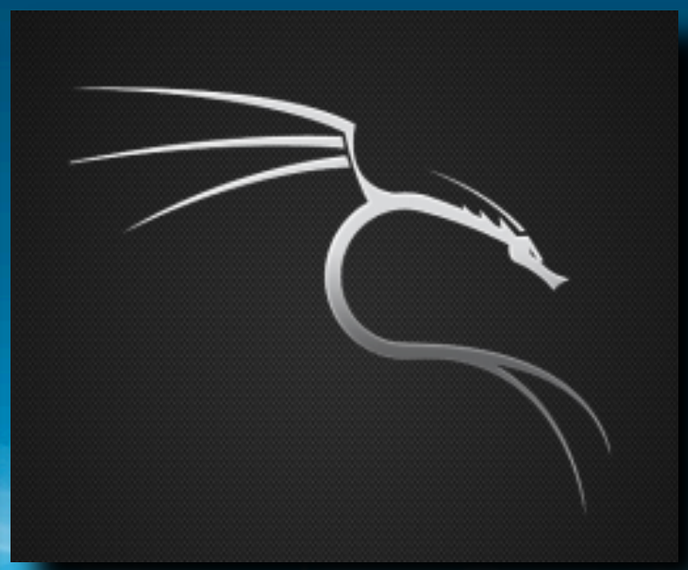














Sun Tzu's *Art of War*

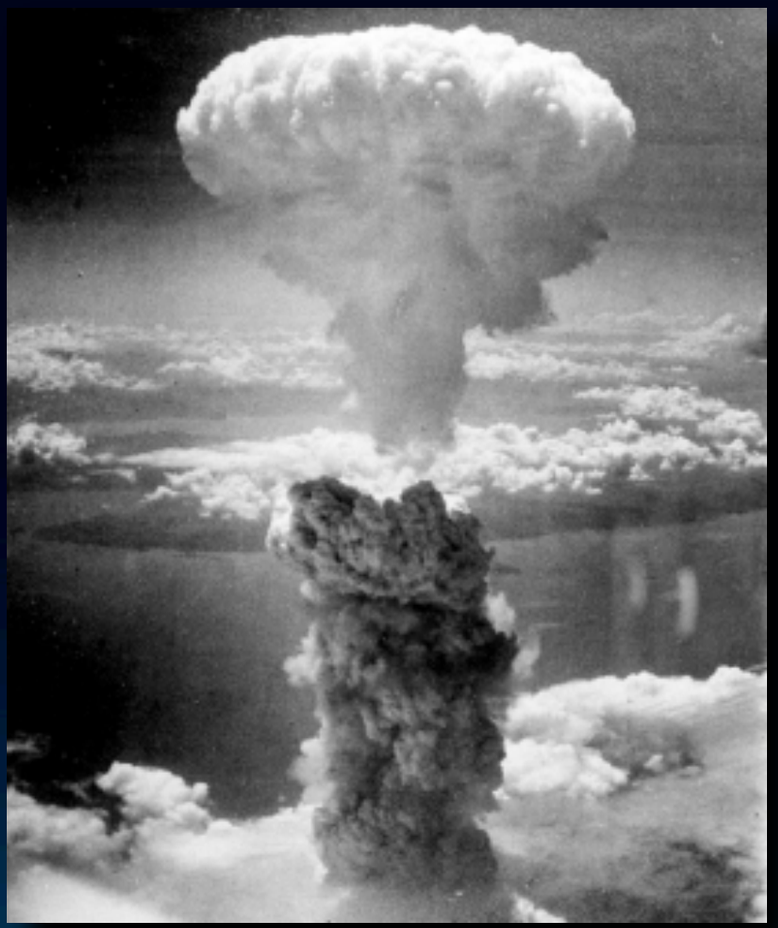
Good … not perfect guide to cyber conflict

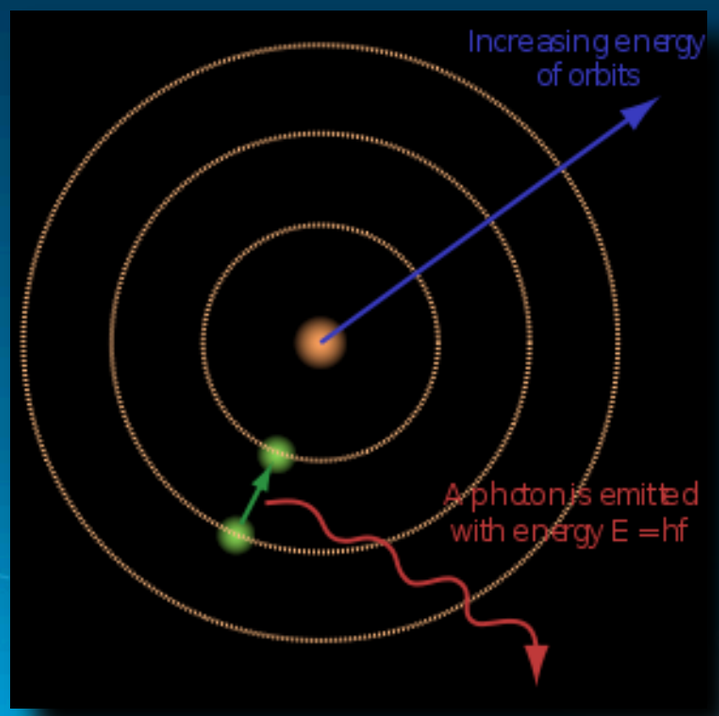
Art of Cyber War

1. Artificial environment
2. Geography changes without warning
3. Physical proximity loses relevance
4. Blinding development of technology
5. Anonymity
6. Few moral inhibitions

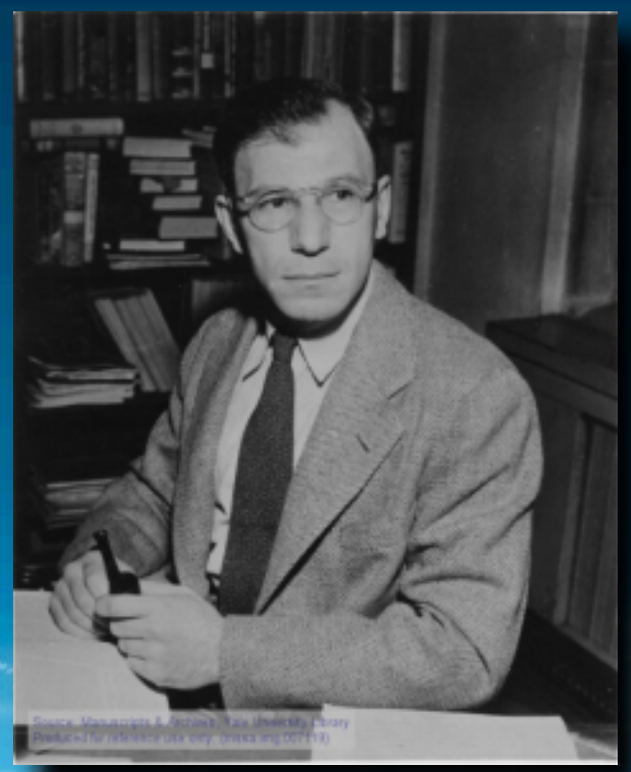







Increasing energy
of orbits
A photon is emitted
with energy E = hf





Cyber Attack Deterrence

Mutually Assured Disruption?

Deterrence options

1. Denial
2. Punishment

Deterrence requirements

1. Capability
2. Communication
3. Credibility






UN




The highest capacity
Flash drive on the market
DT310


HET!





Cyber Arms Control

Model: Chemical Weapons Convention

Proposal: Cyber Weapons Convention

Easy to apply

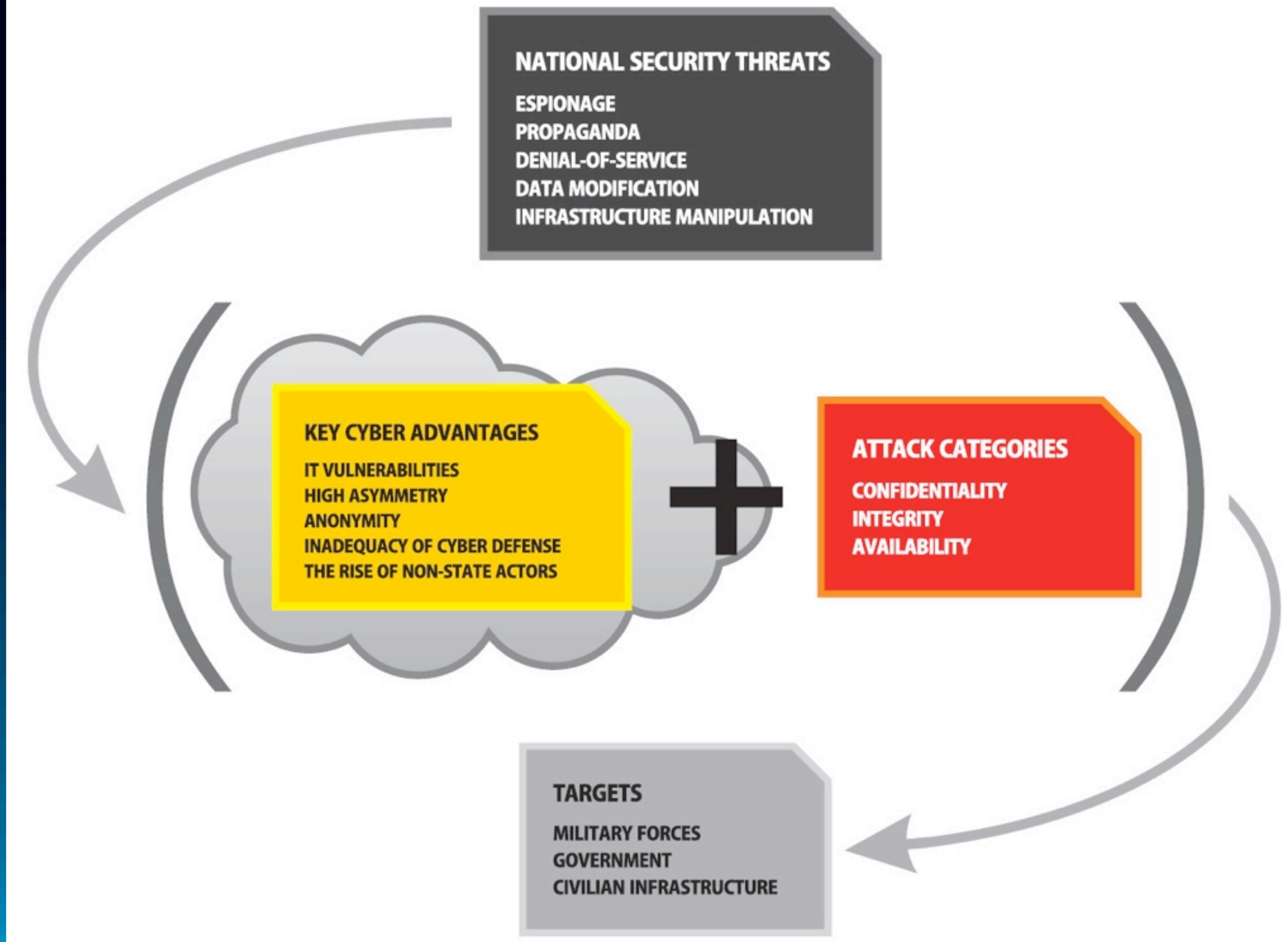
1. Political will
2. Universality
3. Assistance

Hard to apply

1. Prohibition
2. Inspection

The DEMATEL Method

National Security Threats	Cyber Attack Advantages	Attack Categories	Targets	Mitigation Strategies	Overview
Espionage	Myriad IT vulnerabilities	Confidentiality	Military forces	IPv6	Solves some Q's, creates others
Propaganda	Asymmetry	Integrity	Gov/Civ infrastructure	*Art of War*	Good but insufficient
DoS	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				


NATIONAL SECURITY THREATS
ESPIONAGE
PROPAGANDA
DENIAL-OF-SERVICE
DATA MODIFICATION
INFRASTRUCTURE MANIPULATION
KEY CYBER ADVANTAGES
IT VULNERABILITIES
HIGH ASYMMETRY
ANONYMITY
INADEQUACY OF CYBER DEFENSE
THE RISE OF NON-STATE ACTORS
ATTACK CATEGORIES
CONFIDENTIALITY
INTEGRITY
AVAILABILITY
TARGETS
MILITARY FORCES
GOVERNMENT
CIVILIAN INFRASTRUCTURE

NATIONAL SECURITY THREATS

ESPIONAGE
PROPAGANDA
DENIAL-OF-SERVICE
DATA MODIFICATION
INFRASTRUCTURE MANIPULATION

KEY CYBER ADVANTAGES

MYRIAD VULNERABILITIES
HIGH ASYMMETRY
ANONYMITY
INADEQUACY OF CYBER DEFENSE
EMPOWERED NON-STATE ACTORS

THREAT REDUCTION

MITIGATION STRATEGIES

NEXT GEN NET (IPV6)
MILITARY DOCTRINE (TZU)
CYBER ATTACK DETERRENCE
CYBER ARMS CONTROL

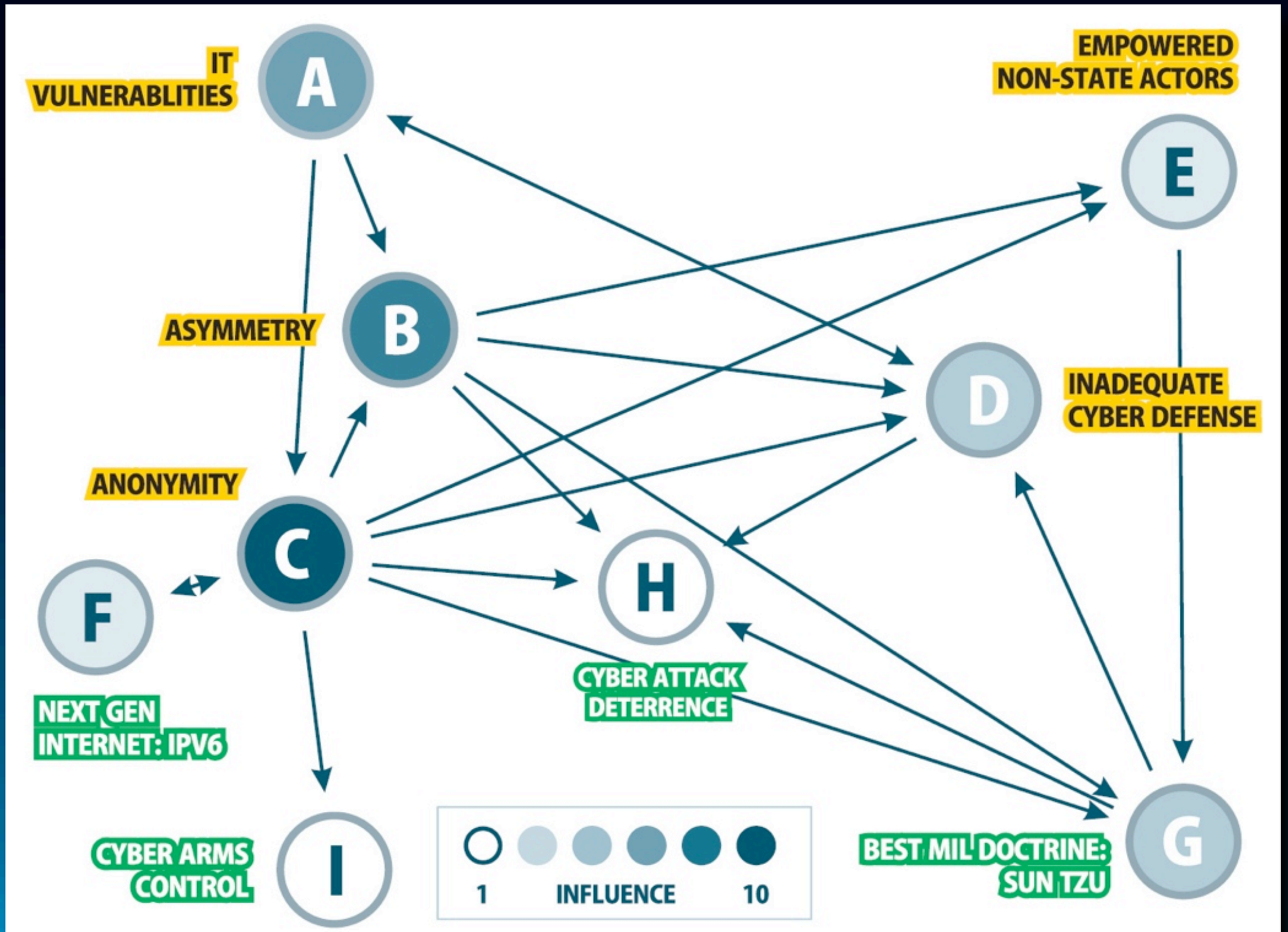


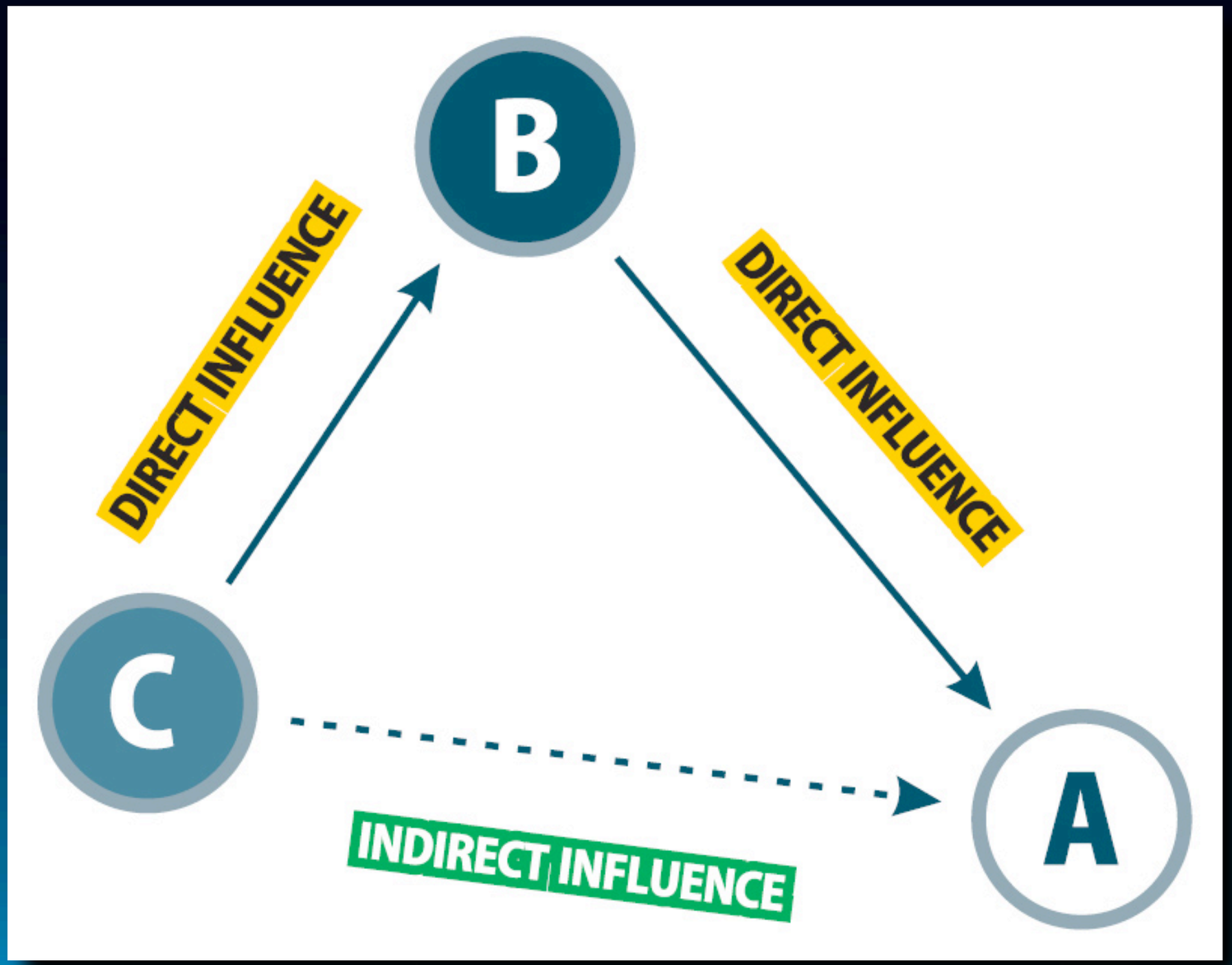
Strategy		Evaluation		
IPv6	>	Increases attribution by lowering anonymity IPsec authenticates, encrypts; not mandatory Long, dangerous transition phase	>	All could help ... But each is only a partial solution
Art of War	>	Sun Tzu good but not perfect Concepts, law behind tech curve Cyber warfare has 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	>	

	DEMATEL "Expert Knowledge" Influence Matrix *X* None = 0 Low = 1 Medium = 2 High = 3 Very high = 4	A IT vulnerabilities	B Asymmetry	C Anonymity	D Inadequate cyber defense	E Empowered non-state actors	F Next Gen Internet: IPv6	G Best mil doctrine: Sun Tzu	H Cyber attack deterrence	I 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	

	Factor	Direct Influence
C	Anonymity	30
A	IT Vulnerabilities	26
B	Asymmetry	24
D	Inadequate Cyber Defense	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

	Factor	Susceptibility to Influence
H	Cyber Attack Deterrence	27
G	Best Mil Doctrine: Sun Tzu	23
D	Inadequate Cyber Defense	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


IT VULNERABLITIES
A
EMPOWERED NON-STATE ACTORS
E
ASYMMETRY
B
D
INADEQUATE CYBER DEFENSE
ANONYMITY
C
F
H
CYBER ATTACK DETERRENCE
NEXT GEN INTERNET: IPV6
CYBER ARMS CONTROL
I
1
INFLUENCE
10
BEST MIL DOCTRINE: SUN TZU
G

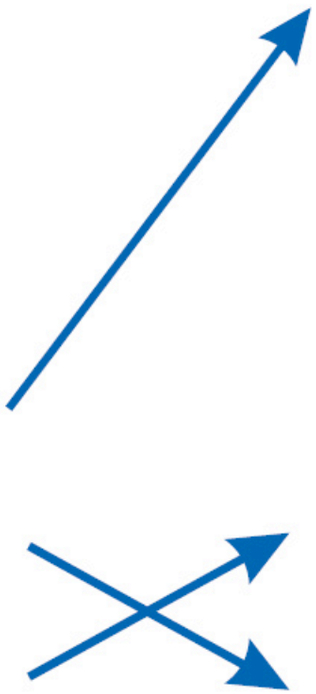

B
DIRECT INFLUENCE
DIRECT INFLUENCE
C
A
INDIRECT INFLUENCE

	DEMATEL "Total Influence" Matrix *T*	A IT vulns	B Asymmetry	C Anonymity	D Inad cyb def	E Non-state act	F Next Gen Net	G Best mil doc	H Deterrence	I 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	

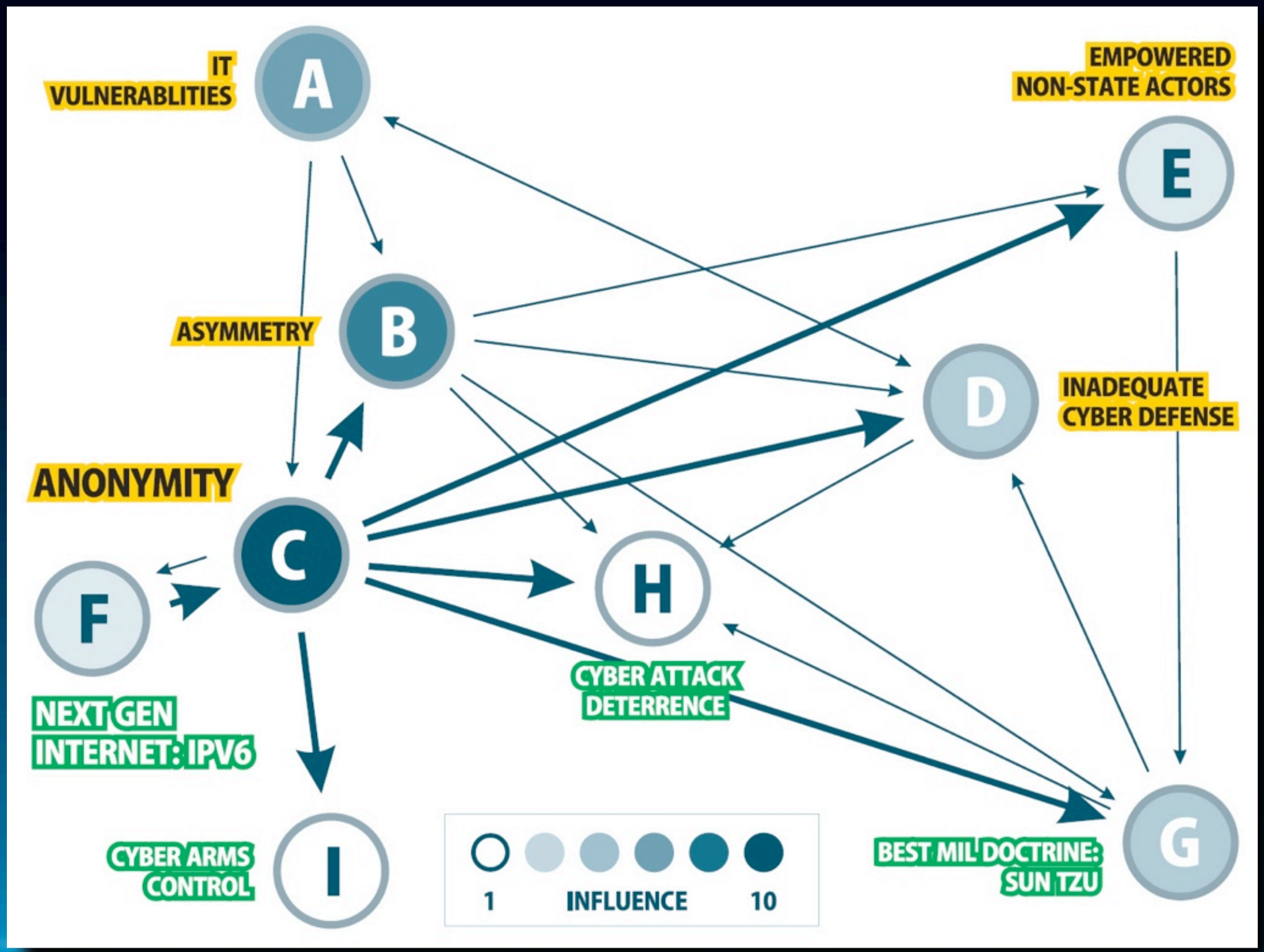
Factor	Direct Influence Index	Indirect Influence Index	Total Influence ***
Anonymity	3.1138	2.1287	5.2425
Inadequate Cyber Defense	2.5176	2.4694	4.9870
Best Mil Doctrine: Sun Tzu	2.2912	2.4797	4.7709
Asymmetry	2.4964	2.2591	4.7555
IT Vulnerabilities	2.8170	1.8572	4.6742
Cyber Attack Deterrence	1.6378	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

	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 Defense	.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

Anonymity	30
IT Vulnerabilities	26
Asymmetry	24
Inadequate Cyber Defense	23
Doctrine: Sun Tzu	21
Empowered Non-State Actors	18
Next Gen Net: IPv6	18
Deterrence	15
Arms Control	14



Anonymity	.9851
IT Vulnerabilities	.9598
Next Gen Net: IPv6	.3369
Asymmetry	.2373
Inadequate Cyber Defense	.0481
Doctrine: Sun Tzu	-.1886
Empowered Non-State Actors	-.2654
Arms Control	-.8496
Deterrence	-1.2636


IT VULNERABLITIES
A
EMPOWERED NON-STATE ACTORS
E
ASYMMETRY
B
D
INADEQUATE CYBER DEFENSE
ANONYMITY
C
F
H
CYBER ATTACK DETERRENCE
NEXT GEN INTERNET: IPV6
CYBER ARMS CONTROL
I
1
INFLUENCE
10
BEST MIL DOCTRINE: SUN TZU
G

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

Conclusion

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

1. Technical
2. Military
3. Political

Author Publications

"From Cambridge to Lisbon: the quest for strategic cyber defense"

In peer-review at Journal of Homeland Security and Emergency Management 1-16 (2011)

"Heading Off Hackers"

Forthcoming in per Concordiam 2(1) 22-27 (2011)

"Sun Tzu and Cyber War"

Cooperative Cyber Defence Centre of Excellence Feb 9, 1-23 (2011)

"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)

Author Publications

"The Challenge of Cyber Attack Deterrence"

Computer Law and Security Review 26(3) 298-303 (2010)

"A Brief Introduction to Cyber Warfare"

Common Defense Quarterly Spring 16-17 (2010)

"The Cyber Threat to National Critical Infrastructures: Beyond Theory"

The Information Security Journal: A Global Perspective 18(1) 1-7 (2009)

Reprinted in Journal of Digital Forensic Practice 3(2) 124-130 (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)

Author Publications

"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)

"Cyberspace and the Changing Nature of Warfare"

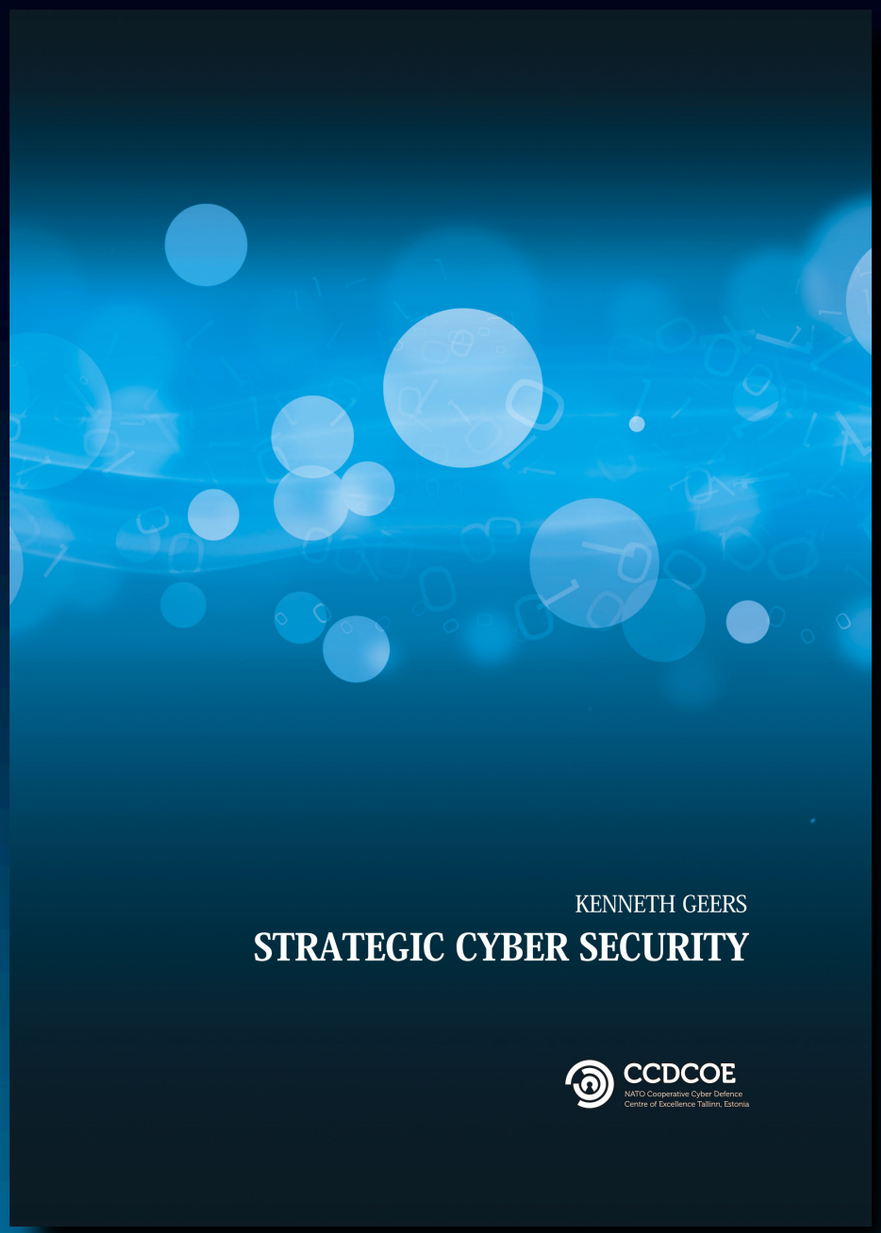
Hakin9 E-Book 19(3) No. 6, SC Magazine (27 AUG 08), Black Hat Japan 1-12 (2008)

"Greetz from Room 101"

DEF CON, Black Hat 1-24 (2007)

"IPv6: World Update" coauthored with A. Eisen

ICIW 2007: Proceedings of the 2nd International Conference on Information Warfare and Security 85-94 (2007)



Strategic Cyber Security

An Evaluation of Nation-State Cyber Attack Mitigation Strategies

Kenneth Geers

NCIS Cyber SME

Free download:

ccdcoe.org/278.html