DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

DEC 2 0 2018

Michael Martelle
The National Security Archive
Gelman Library, Suite 701
2130 H Street, N.W.
Washington, D.C. 20037

Dear Mr. Martelle,

Thank you for your September 9, 2018 Freedom of Information Act (FOIA) request for the briefing on operational strategy given by the Combined Action Group in October 2016.

As the initial denial authority, I am partially denying portions of the document under 5 U.S.C. §§ 552(b)(1) and (b)(3). The denied portions include classified national security information under the criteria of Executive Order 13526 (labeled as (b)(1)) and personally identifying information regarding personnel assigned to a sensitive unit exempt from disclosure under 10 U.S.C. § 130b (labeled as (b)(3)). U.S. Cyber Command is a sensitive unit.

If you are not satisfied with our action on this request, you may file an administrative appeal within 90 calendar days from the date of this letter by U.S. mail or email. If you submit your appeal in writing, please address it to ODCMO, Director of Oversight and Compliance, 4800 Mark Center Drive, ATTN: DPCLTD, FOIA Appeals, Mailbox #24, Alexandria VA 22350-1700. If you submit your appeal by email please send it to OSD.FOIA-APPEAL@mail.mil. All correspondence should reference U.S. Cyber Command case tracking number 19-R011.

Additionally, you may contact the Office of Government Information Services (OGIS), which provides mediation services to help resolve disputes between FOIA requesters and Federal agencies. Contact information is 8601 Adelphi Road – OGIS, College Park, MD 20740-6001. OGIS may also be reached at ogis@nara.gov, 202-741-5770, and 1-877-684-6448.

Sincerely,

Ross A. Myers

ROSS A. MYERS
Rear Admiral, U.S. Navy
Chief of Staff

How understanding cyberspace as a strategic environment should drive cyber capabilities and operations

(b)(3) Sec. 130b Combined Action Group, US Cyber Command & NSA

The overall classification of this briefing is: ~~TOP SECRET//SI//NOFORN~~

Classified By: (b)(3)
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: <20411128>

(U) Strategic capability, effect, environment

- (U) Strategic capability & effect = impact on the systemic distribution of power, either regionally or globally.
- (U) Nuclear weapons, because of their immediate systemic impact, collapsed the difference between capability and effect.
- (U) Nuclear = Strategic; but that is not the case in traditional conventional or cyber environments.
- (U) Strategic environments = dominant technology creates a structure that reinforces core conditions and fundamental dynamics.

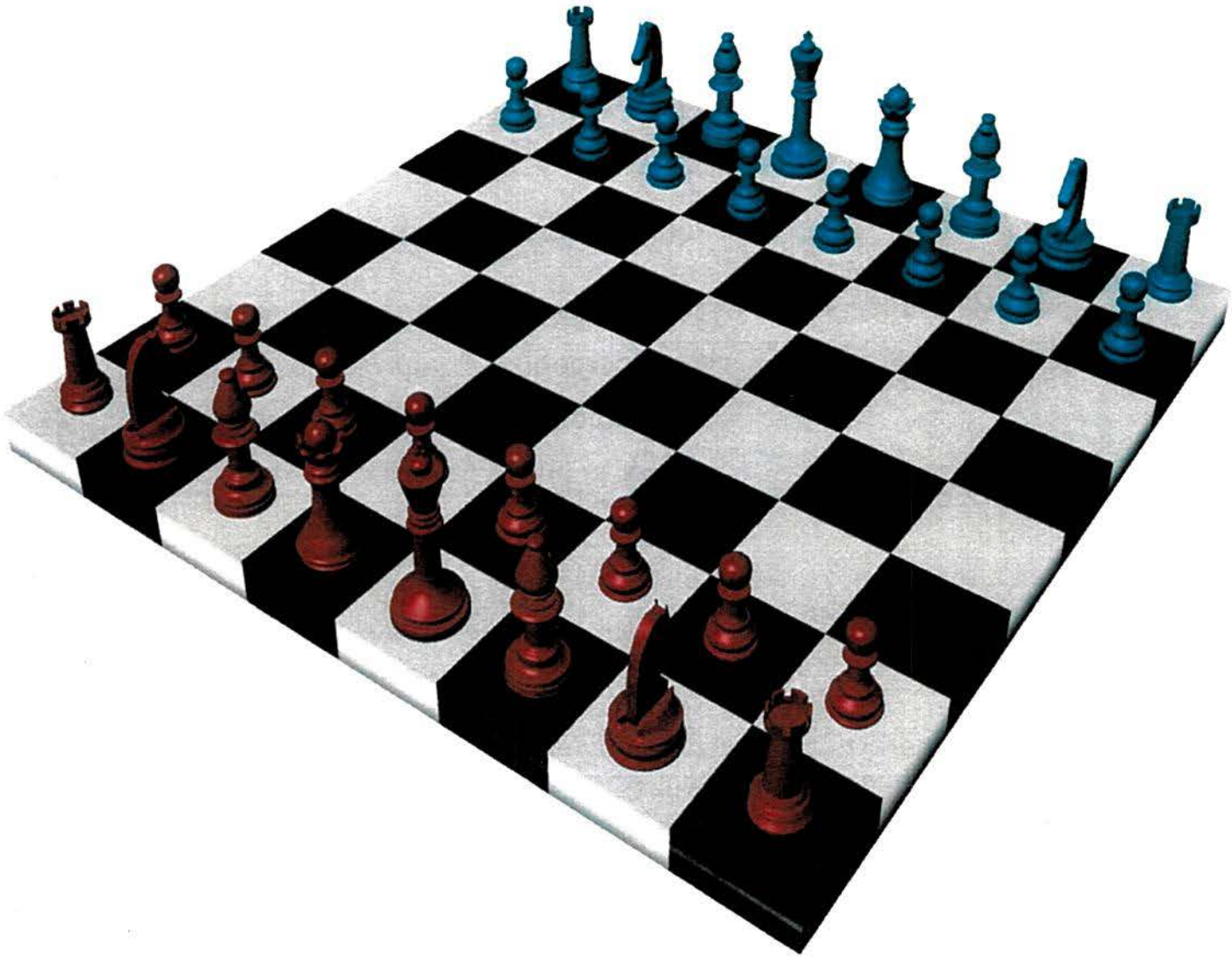
(U) BLUF: Nuclear v. Cyber Thinking

- (U) Misalignment between policy and the strategic environment actually has a strategic impact.
- (U) We are self-constraining through a focus on cyber deterrence as the strategic frame.
- (U) This has cleared space for increased adversarial maneuver and capability development in support of strategies of cyber persistence.
- (U) We need to adopt the process of nuclear thinking, not the output of that thinking...Nuclear thinking is narrowing cyber capabilities' relevancy.

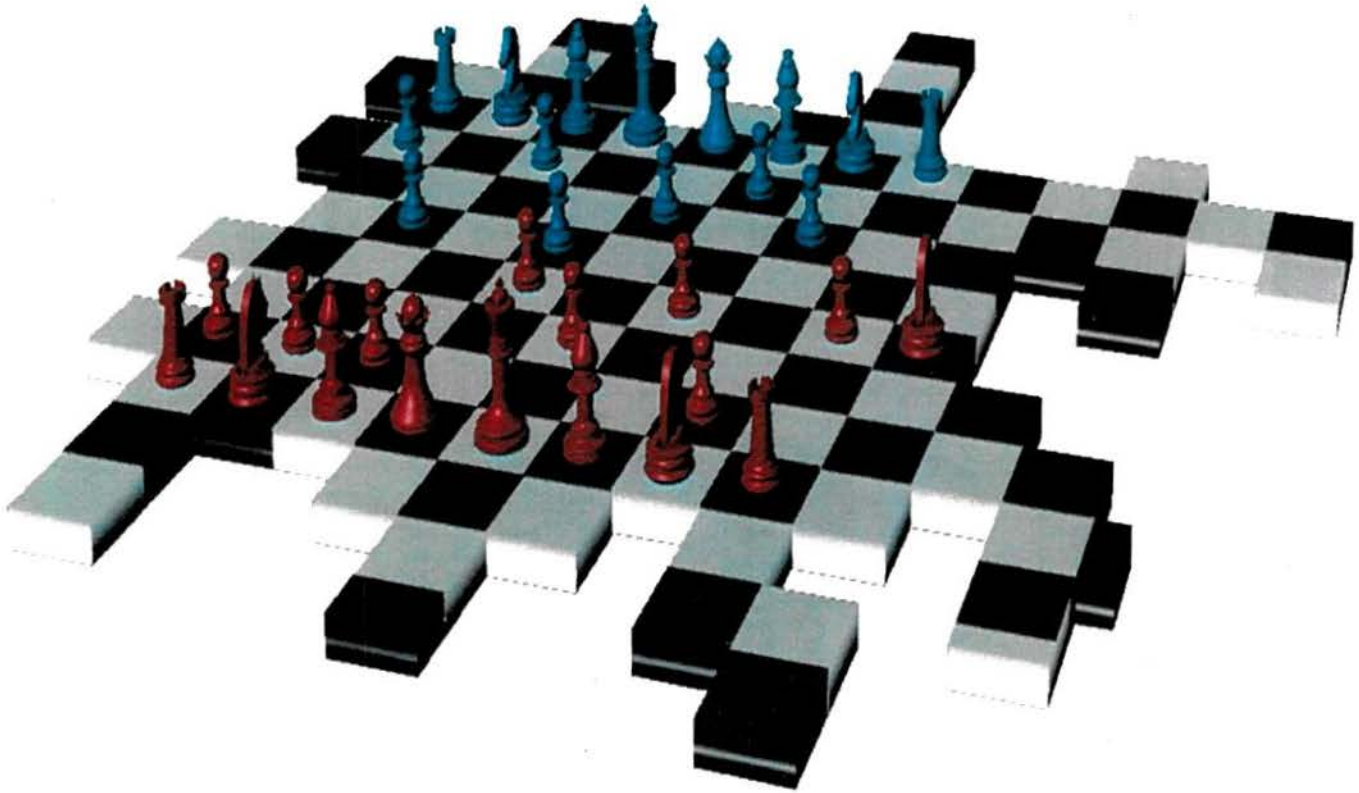
(U) The Incontestable Effect

Unclassified	Nuclear Strategic Environment
Technological Imperative	Pure offense dominance
Core Condition	Assured destruction
Intervening Variable(s)	Mutual possession of second strike capability
Dominant strategic dynamic	Deterrence
Locus of action	Initiative is relinquished to the other side
Security rests…	In the decision calculus of the adversary
Core strategic question	How do I secure when I cannot defend?
Measure of Effectiveness	Absence of specified adversarial action
Decision-making model	Centralized, one big decision, one time Time is condensed
Crisis management	Leaving the last clear chance to avoid catastrophe to the adversary
Escalation dynamics	National interests advanced through deescalated outcome
Capabilities development	Hold at risk strategic; exotic; expensive; one-off

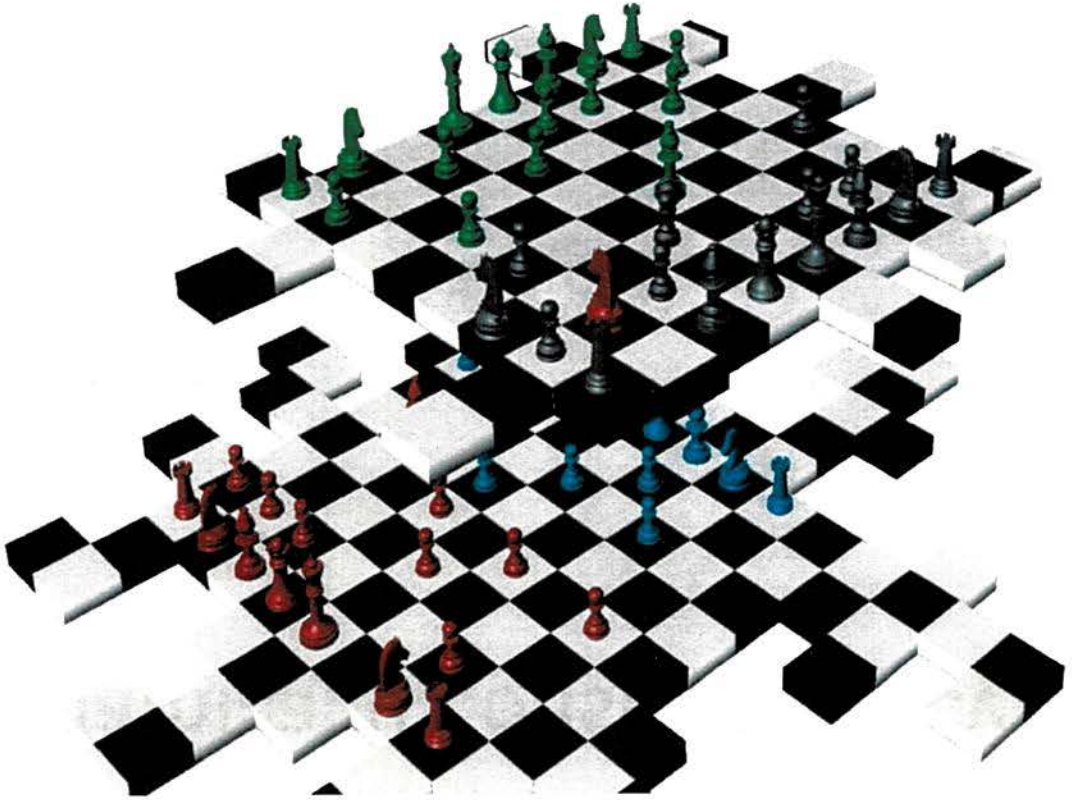
Nuclear strategic contest



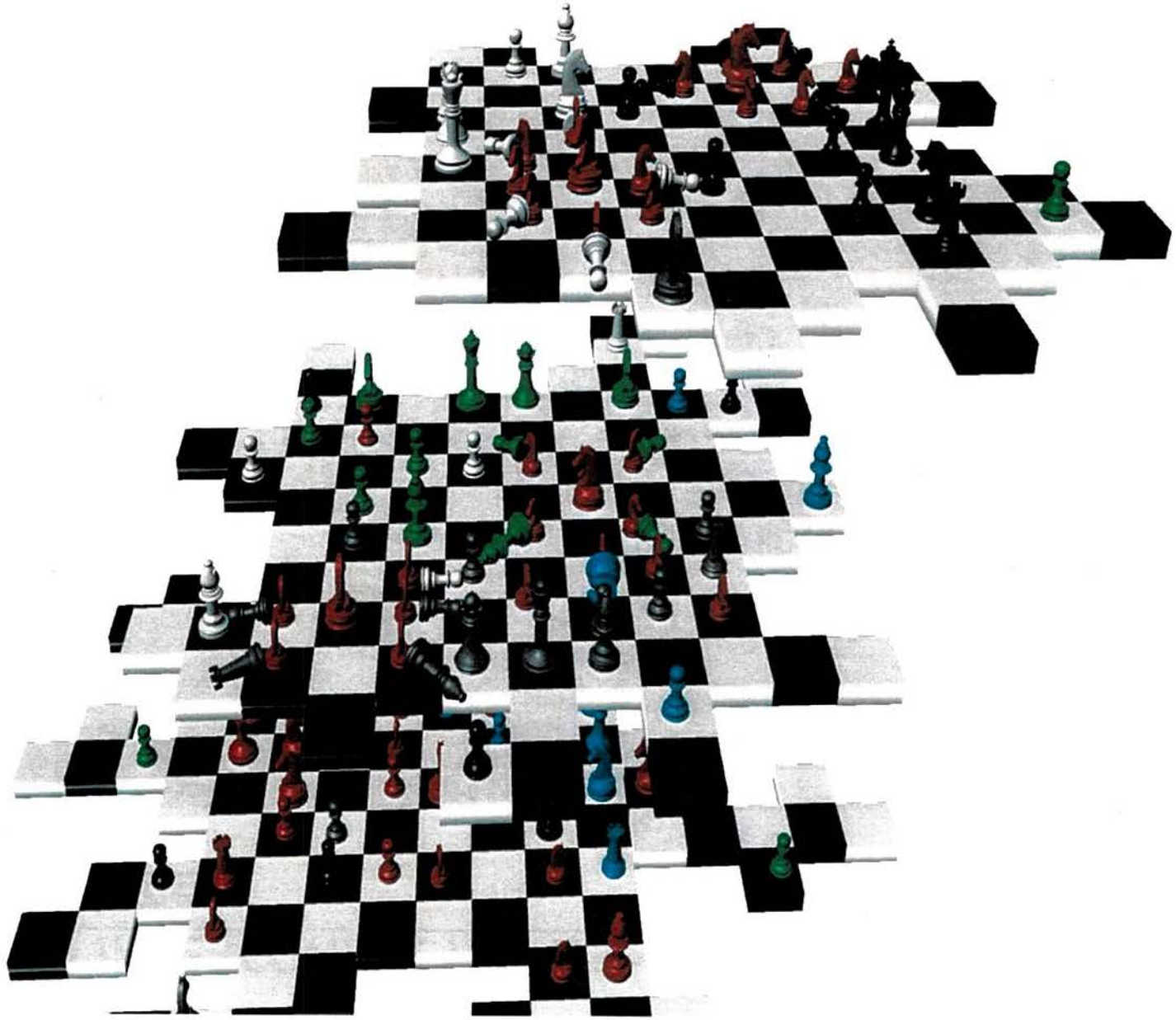
Dynamically Constructed Cyber terrain



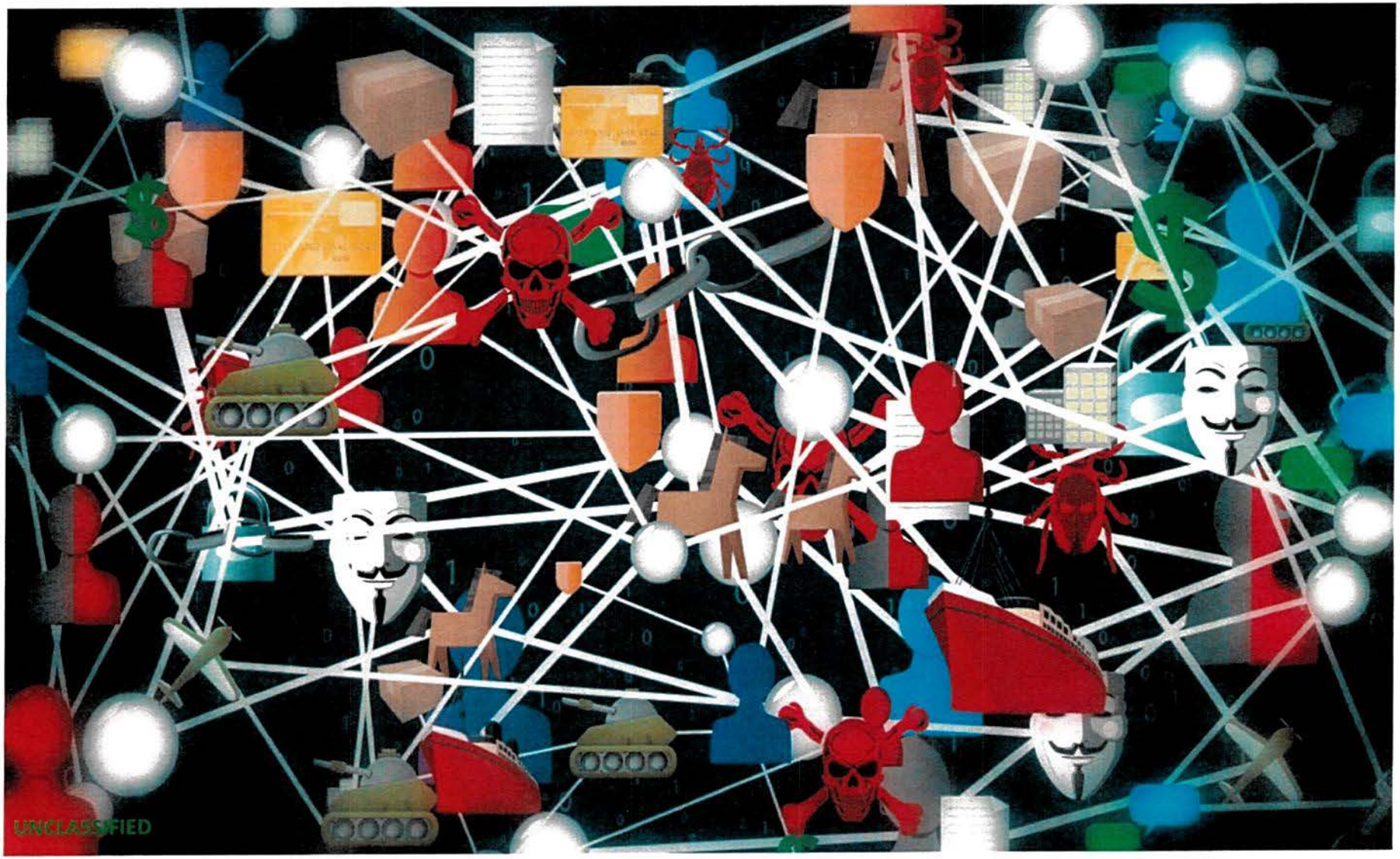
Constant Contact



Cyberspace is an Interconnected domain



(U) The INTERCONNECTED Threat & Opportunity Environment

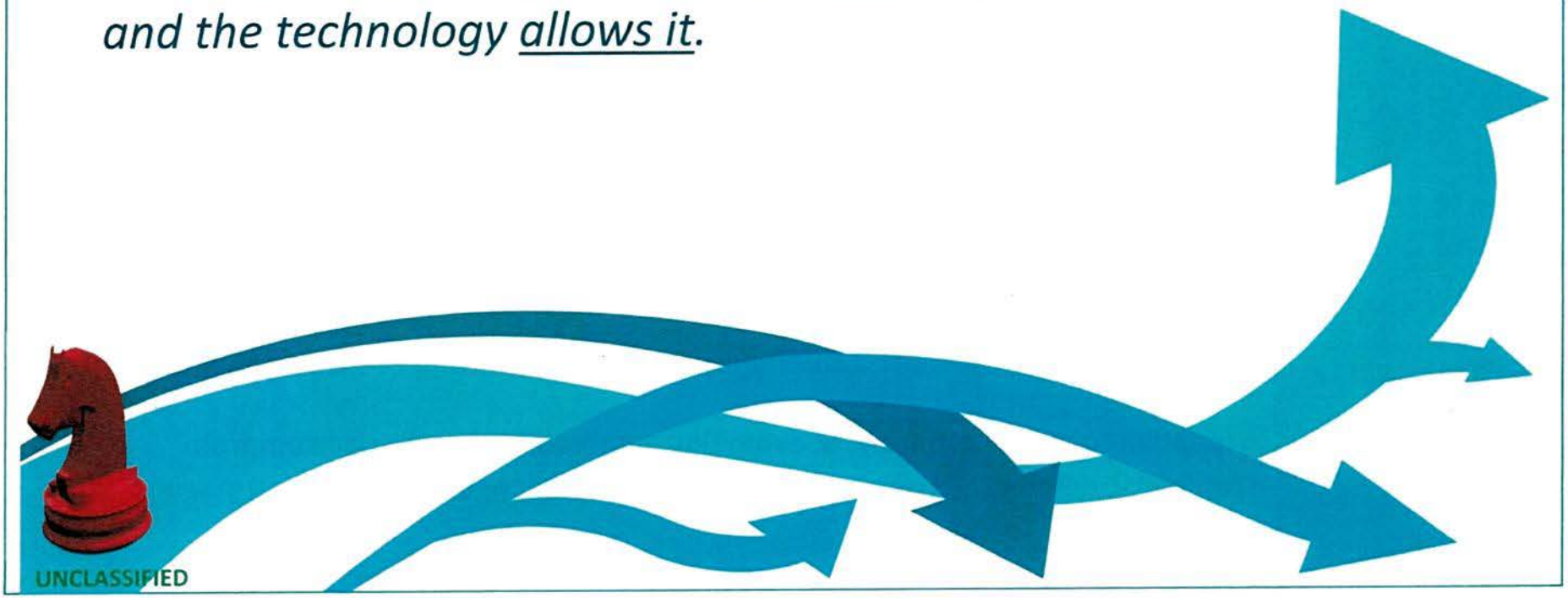


Unclassified	Cyber Strategic Environment
Technological Imperative	Interconnected
Core Condition	Constant Contact
Intervening Variable(s)	Dynamically constructed terrain;
Dominant strategic dynamic	Persistence
Locus of action	Initiative must be seized and retained
Security rests…	In the effective grappling over cyber initiative
Core strategic question	How do I secure when I am in constant contact with the adversary, ally, business sector and individuals all of whom are operationally persistent?
Measure of Effectiveness	Anticipation of the exploitation of cyber-related vulnerabilities
Decision-making model	Constant, Conditional from the edge up; Time is crushed
Crisis management	Cyber compellence at phase 0; cross domain reliant
Escalation dynamics	National interests advanced through winning or supporting deescalation outcome
Capabilities development	Adaptive to stay out in front of exploiting vulnerabilities: full spectrum from resiliency, defense, active defense, offense (tactical, operational and strategic)

(U) The Technology is adaptive and iterative; the Terrain is constantly shifting

(U) Operational Persistence is a systemic condition of continuous willingness and capacity to seek the initiative.

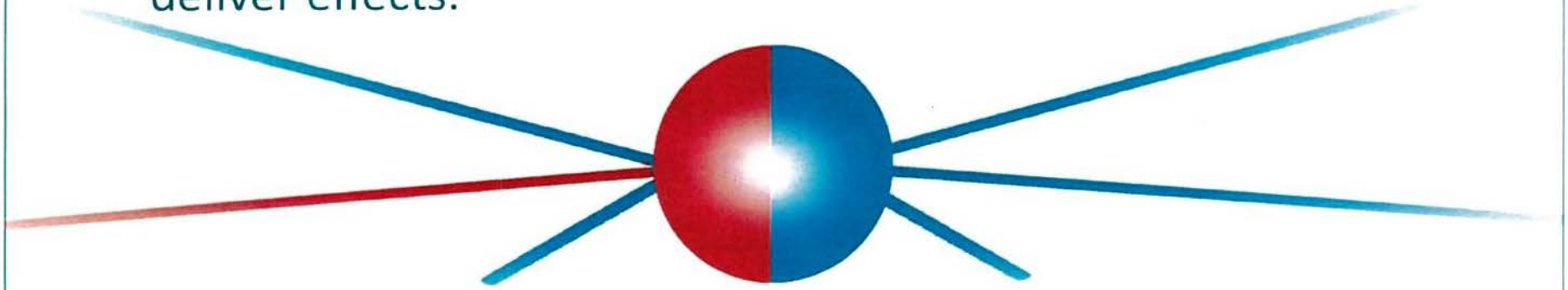
(U) The terrain of cyber space encourages persistence and the technology allows it.



(U) Thinking Differently to Organize, Plan, & Operate Differently

Persistence is the 180 degree opposite of deterrence.

Seize the cyber initiative through maneuver within our own systems, in neutral systems, and into adversary systems with operations that deny nodes to actors as terrain to be used, while we use those same nodes ourselves to deliver effects.



(U) Cyber Initiative (defined)

- (U) the technical, tactical, and operational outcome of **effective anticipation of the exploitation of cyber-related vulnerabilities**.

- (U) The anticipation enables both the prevention of exploitation by adversaries and the leveraging of exploitation by the United States.

  - (U) Tactically and operationally denying, disrupting, seizing and retaining the cyber initiative includes the full range of activities included in cyber resiliency, defense, active defense, CNE, offense.

(U) Cyberspace superiority

- (U) the sustained technical, tactical, and operational outcome of effective anticipation of the exploitation of cyber-related vulnerabilities across the interconnected domain of cyberspace that permits the secure, reliable conduct of operations at a given time and place without prohibitive interference by an adversary. (revising JP 1-02 language)

- (U) Cyberspace superiority is sustained cyber initiative.

(U) Deterrence and cyber operations

- (~~S//REL TO USA, FVEY~~) "The proposed operational concept employs planning principles based on strategic deterrence and escalation control strategy through development of (b)(1) Sec. 1.4(a) (b)(1) Sec. 1.4(a) (b)(1) Sec. 1.4(a) that readily support strategic deterrence and escalation control; and which can synchronize with WOG strategic deterrence and escalation control efforts. USCYBERCOM will develop and integrate (b)(1) Sec. 1.4(a) (b)(1) Sec. 1.4(a) (b)(1) Sec. 1.4(a) to impose costs, deny benefits, demonstrate resiliency, and encourage adversary restraint."
  - (~~TS//NF~~) USCYBERCOM COMMANDER'S ESTIMATE: CYBER MISSION FORCE (CMF) BALANCING STRATEGY AND STRATEGIC DETERRENCE AND ESCALATION CONTROL FRAMEWORK (TS//NF) 22 Oct 2015

(U) Russian strategic use of cyber capabilities

- (U) Overall objective= shift the systemic distribution of balance by undermining faith in domestic democratic and European-wide institutions.
- (U) Cyber-enabled social media manipulation/Cyber-amplification
- (U) Cyber attacks on legitimacy of elites and electoral processes. (German Parliament/CDU; DNC/Clinton Campaign; Ukraine election Commission)
- (U)"Firehose of Falsehood" model: high-volume, multichannel, rapid, continuous, repetitive, agile, targeted. [1]
- (U) What is U.S. strategic counter-capability?

(U)China Sinosphere

- (U) Supports both larger PRC goals of economic development and information control.[1]

- (U) Strategic goal to erode U.S. advantage in cyberspace
  - (U) Harness the PRC cyber community – world's largest (>647 million) – as "throw weight" in demanding foreign businesses operating in PRC comply with laws, regulations.
  - (U) Build and support PRC technology firms
  - (U) Construct, operate information networks in developing world
  - (U) Promote PRC concepts of cyber governance and cyber security in international organizations
  - (U) Leverage position as world's largest manufacturer of Information-Computer Technology (ICT) equipment to shape global engineering and design standards while marketing its indigenous systems

(U) Post 2015 September Agreement Activity

- (~~TS//SI//REL~~) (b)(1) Sec. 1.4(a)

(b)(1) Sec. 1.4(a) Chinese cyberactors,

(b)(1) Sec. 1.4(a)

(b)(1) Sec. 1.4(a)

(U) Post 2015 September Agreement Activity

- "(~~TS//SI//NF/FISA~~) In particular, Chinese cyber

(b)(1) Sec. 1.4(a)

  - *Comment: If the Chinese* (b)(1) Sec. 1.4(a)

(b)(1) Sec. 1.4(a)

(U) Strategies of Cyber Persistence

- (U) Revisionist states understand that Cyber capabilities and operations can effect the systemic distribution of power.

- (U) They are engaged in a broad integrated application of cyber capabilities to undermine American power.

- (U) How can the U.S. leverage cyber as a counter-strategic capability?

  → It must broaden its application and framing beyond a deterrence-centric narrow box and embrace interconnectedness, master constant contact, and persist in sustaining the cyber initiative.

(U) Starkly Different Strategic Environments

Unclassified	Nuclear Strategic Environment	Cyber Strategic Environment
Technological Imperative	Pure offense dominance	Interconnected
Core Condition	Assured destruction	Constant Contact
Intervening Variable(s)	Mutual possession of second strike capability	Dynamically Constructed terrain;
Dominant strategic dynamic	Deterrence	Persistence
Locus of action	Initiative is relinquished to the other side	Initiative must be seized and retained
Security rests…	In the decision calculus of the adversary	In the effective grappling over cyber initiative
Core strategic question	How do I secure when I cannot defend?	How do I secure when I am in constant contact with the adversary, ally, business sector and individuals all of whom are operationally persistent?
Measure of Effectiveness	Absence of specified adversarial action	Anticipation of the exploitation of cyber-related vulnerabilities
Decision-making model	Centralized, one big decision, one time Time is condensed	Constant, Conditional from the edge up; Time is crushed
Crisis management	Leaving the last clear chance to avoid catastrophe to the adversary	Cyber compellence at phase 0; cross domain reliant
Escalation dynamics	National interests advanced through deescalated outcome	National interests advanced through winning or supporting deescalation outcome
Capabilities development	Hold at risk strategic; exotic; expensive; one-off	Adaptive to stay out in front of exploiting vulnerabilities: full spectrum from resiliency, defense, active defense, offense (tactical, operational and strategic)