The Dynamics of Cyber Conflict

Robert Jervis and Jason Healey

That we live in a cyber era is an inescapable aspect of international security. Yet the study of cyber conflict – and indeed the policy responses to it – have lagged the practice of states which every year are pushing their cyber capabilities and conducting more operations with ever-increasing audacity.

"Dynamics" here means the mix of physics, attributes, doctrines, and dogmas which characterize conflict and our understanding of it. It is what we tell ourselves is true about conflict. For example, aircraft at the higher altitude have a tremendous advantage; many believe the best defense against a tank is another tank; and fleets can be used to control key maritime choke points.

Such dynamics for cyber conflict are hidden and indirect; a few are fixed while others change over time. Some are based on often-unchallenged assumptions or differ at the tactical, operational, and strategic levels.

Many national cyber policies, for example, will begin with a boilerplate nod to such dynamics: the Internet is "borderless," cyber-attacks can happen at "network speed" and be hard to attribute and deter, or that the low barriers to entry allow non-state actors to gain state-like offensive capabilities. But since there are so many dynamics, and little work to structure and analyze the entire set, it has been easy for strategists and academics to, unconsciously or not, cherry pick some and ignore others.

Ongoing research at Columbia University (funded by the Minerva program of the US Department of Defense) examines several key questions, starting with what is the complete set of dynamics of cyber conflict? The research is particularly well suited to analyzing the new U.S. recognition of cyber conflict as a state of "persistent engagement" and the resulting policy of "forward defense."

This short brochure summarizes some of the research to date, introducing a more comprehensive and structured approach. The following two pages includes a table including the dozens of dynamics (section 1) and two ways the dynamics can be categorized (section 2). Section 3 summarizes which are perhaps most important while section 4 examines feedback loops by which particular actions or policies might be intentionally or unintentionally magnified, possibly inducing adversaries to more aggressive behavior over time. Section 5 includes key questions for further study. The back page focuses exclusively on forward defense.

SIPA Initiative on Cyber Risk

This research is part of a series of the Initiative on Cyber Risk at the School of International and Public Affairs at Columbia University. Recent scholarship and programs include:

Building a Defensible Cyberspace: This report, by the New York Cyber Task Force, drew lessons from 50 years of defensive innovations, across technology, operations and policy. The goal is to give defenders the greatest advantage over attackers at the greatest scale and least cost.

Cyber Risk to Financial Stability: This research, done in concert with SIPA's Initiative on Central Banking and Financial Policy, is the most comprehensive analysis of how cyber risks might impact financial stability.

Dynamics and History of Cyber Conflict: Despite a decades-long history of cyber conflict, there has been little effort to rigorously assess the dynamics and their interactions. SIPA's work in this space includes research, instruction to students, and convening events like the Workshop on the State of the Field of Cyber Conflict and Bridging the Gap workshop, for international relations scholars, both in partnership with the Cyber Conflict Studies Association. A related project seeks to build an analytical framework to assess if the new US cyber deterrence posture is suppressing or encouraging attacks.

For Office of Naval Research under the OSD Minerva program grant number N00014-17-1-2423

Understanding the Dynamics of Cyber Conflict

1 There are dozens of interrelated dynamics of cyber conflict. We have identified those below:

The "dynamics" are the mix of physics, attributes, doctrines, and dogmas that characterize conflict in cyberspace. These are the range of what we tell ourselves to be true about such conflicts and how to prevail in them.

Tactically moves at "network speed"	Attacker advantage	Difficult to deter
Slower at operational, strategic levels	Difficulty of quick or exact attribution	Defense success does not discourage attackers
Cyberspace is a scale-free network	Hard to directly observe	Difficult to warn of attacks
Cyberspace is human-made and adaptable	Capabilities are transitory and have hard-to-predict effects	Signaling intent is problematic
Cyberspace is unfathomably complex	Adversary forces in constant contact with few if any operational pauses	Likely to be first-strike weapons
Cyberspace contains inherent vulnerabilities	Immediate, intercontinental proximity to national sources of power	Surprise is more important
Low-impact and reversible effects of capabilities	Advantage comes from use of capabilities, not possession	Easy for nations to leverage proxies
Attack is lesser included case of espionage	Adversaries routinely use capabilities mostly below level of armed conflict	Offense & defense similar, inform one another
Fast pace of technological change	Low barriers to entry	Conceptual confusion and lack of precise definitions
Universal interconnection and dependence	Superiority is fleeting	Insufficient and competing authorities
Permissionless innovation and connection	Capabilities are substantially cheaper than in other domains	Difficult command and control
Fuzzy borders	Capabilities can be rapidly regenerated	Heavily classified
Tied to the physical world	Attacks might lead to catastrophic effects	Tactical engagement is basic unit of analysis
Ease of copying information (and capabilities)	Tactical success tied to agility and initiative	Conflict escalates horizontally and vertically within cyberspace but not yet out of it
Dominated by private sector	Strategic success possibly more tied to audacity and initiative	Cyber conflict may invite escalation, miscalculation and instability

2 Two groupings of dynamics

That's obviously too many dynamics to process. These can more usefully be grouped in two ways. The first sorts them into related themes:

- **Speed and Agility:** This set of dynamics emphasizes the tactical speed of the domain and need for agility
- **Universal Vulnerability:** This is not just a "warfighting" domain as the entirety of modern society and economy are dependent and vulnerable
- **Confusing, Uncertainty, and Hidden**: Little of cyber conflict is straightforward, possibly feeding mistake and miscalculation
- **Perceived Lack of Restraint**: Most adversaries seem sure others are unfairly getting the better of them.
- **Covert Usability Leads to Persistent Engagement**: Adversary forces and capabilities are engaged every day against each other
- **Outsize Role of Non-State Actors on Defense as Well as Offense**: In many countries, the private sector is in the front lines of conflict and often have more capabilities than governments
- **Early Use in Surprise Attack**: Adversaries may open a conflict with a cyber attack or only attack because cyber gives a perceived first-strike advantage

The second sorts in relation to each other:

- **Fundamental and Fixed**: Some dynamics – like network speed -- are like "physics" in that they can't be easily changed, just accepted
- **Fundamental but Flexible**: Other dynamics are less permanent and might change through changes in technology or decisions by adversaries. Attribution has, for example, become far easier
- **Derivative**: Other dynamics are dependent on more fundamental dynamics
  - Some are **implications** of fundamental dynamics. For example, the difficulty of deterring attacks stems from many other dynamics like covert usability and difficulty of attribution
  - Others are **self-imposed**. Extensive classification and conceptual confusion happens in our own heads, not the networks
  - Many dynamics are **conditional on adversary behavior** and may change overnight. Cyber conflict might escalate into kinetic conflict due to adversary choice, mistake, or miscalculation

Robert Jervis and Jason Healey, Columbia University SIPA

3 Which dynamics are most important?

These two dynamics are **most different from conflict in other domains** (and therefore furthest from traditional military perspectives):

- Covert usage leads to persistent engagement
- Role of the private sector

Two others are **least understood** and therefore very dangerous as we're likely to underestimate the impact:

- Likelihood and impact of surprise attack
- Role of escalation, especially with respect to feedback loops, mistake, and miscalculation

5 Questions for further study

1. Will forward defense impose more positive or negative feedback?
2. How policymakers can know if it is working as advertised?
3. How can we keep a lid on a never-ending competition in cyberspace with the forces of nuclear armed states?
4. Will US have to decide between stability and superiority?
5. How does this all change civil-military relations?
   - Conflict is being fought in private sector networks and on IT depended on by American society and economy.
   - In order to win in its preferred fashion, the US military demands few political constraints during wartime. How does that work when conflict never ends?
   - The Internet was engineered with liberal principles at odds with military mindset: no hierarchy, no privileged role for states, no clear lines between military and civilian

4 Feedback loops are perhaps the most concerning, overlooked mechanism

Negative feedback *counters* an initial stimulus, returning the system to equilibrium: driving in a stable car with good tires on a dry road.
Positive feedback *amplifies* a signal, pushing the system toward instability: driving a clunker with lousy tires on an icy road.
Forward defense and persistent engagement have three kinds of feedback loops.

A) "On Net" feedback is most immediate:

- **Friction**
  - Operations to "intercept and halt cyber threats" and "degrade [adversary] infrastructure" will impose costs and directly frustrate adversary operations, imposing negative feedback [Nakasone]
- **Tacit bargaining**
  - As adversaries seek to "outmaneuver each other to achieve an advantage," the "interactive process will result in tacit understandings among and between adversaries of what behaviors are acceptable and unacceptable in cyberspace [Harknett & Fischerkeller]
- **Tit-for-tat**
  - Generates dangerous positive feedback if nations felt the need for equivalent retaliation (or rather, aim to "be a little more than proportionate") to incoming cyber attacks [Baker]

B) "Off Net" feedback happens over longer timescales:

- **Deterrence**
  - "Over time, if you push back, hopefully you'll get a deterrence effect … [Adversaries will] sense that this is not worth the energy … to try to do x, y or z" [Goldman]
- **Perceived restraint and adherence to norms**
  - If states perceive other states are generally ignoring norms, they are less likely to see benefit of themselves complying leading to negative feedback
- **Emotion and cognitive biases**
  - If an adversary is afraid of provoking a kinetic response or challenging a rival in cyberspace, emotion will dampen conflict. But anger and fear can encourage miscalculation and mistakes, sparking conflict
- **Posture and organizational dynamics**
  - Overlap in their effects, mostly with positive feedback. Declaring "offense is the best defense" may lead adversaries to adopt same posture. Once created, offensive cyber commands will push to conduct offensive operations

C) Feedback to/from the larger system:

- Cyberspace is dominated by the private sector
- Cyberspace is not (just) a military domain but increasing underpins everything
- Even if "forward defense" works as expected, impact on Internet, larger national and economic security goals may be significant

Issue: We don't know if cyber conflict/competition likely to be more sensitive to positive or negative feedback

All positive-feedback systems "are characterized by a self-impelled 'switch' or discontinuity between two extreme states" [Golding, 1994]. There could be a tipping point where cyberspace is far, far more insecure than today. US may not be able to balance superiority and stability

Dynamics of Persistent Engagement and Forward Defense: The United States is in the midst of its most resounding policy shift on cyber conflict to date, with profound (and poorly understood) implications. The National Cyber Strategy states that a "now-persistent engagement in cyberspace is already altering the strategic balance of power." This strategy embraces a new operational model: since US cyber forces are in constant contact with adversaries, then it is an imperative for them to "defend forward" to "persistently engage" to contest these adversaries.

The process of understanding and dealing with these risks will not be completed in weeks or months, but, as with the nuclear age, over years and decades. There is no conflict termination, only a string of engagements, operations, and campaigns. **This fight will not be just "persistent," but permanent**, a never-ending conflict between United States, Russia, Iran, and China.

This more engaged forward defense is intended to cause "friction" to reduce the resources adversaries can commit to offense, disrupting their ability to attack the US. It is also meant to affect their *willingness* to do so, by demonstrating "to adversaries that the cost of their engaging in operations against us is higher than they want to bear," in the words of National Security Advisor John Bolton. This can be thought of as "negative feedback," to bring conflict back to historic norms. This chain of cause and effect is presented in the figure to the right.

But **cyber conflict might not work this way**. Capabilities are relatively cheap and easy to regenerate so adversaries may be able to easily replace any resources lost to U.S. friction. And more U.S. offensive cyber operations might instead cause "positive feedback" if adversaries see a challenge to rise against, rather than one from which to back away. As one of us (Jervis) wrote in 1997, "a failure to anticipate positive feedback is one reason why consequences are often unintended" in international affairs, as unseen effects can rapidly snowball.

Implied Causal Logic of Persistent Engagement

Problem

1. Adversaries are conducting attacks to **destabilize the United States** (and its allies) and **erode sources of national power**;

Method

2. US cyber forces must **defend forward** against these threats and maintain persistent presence;
3. To achieve advantage, US cyber forces must face **reduced operational constraints** to act on fleeting opportunities;
4. With persistent presence, the United States can "**intercept and halt cyber threats**,"
5. Persistent presence will **improve US defenses** as DoD observes adversary behavior and warns targets;
6. Together, these actions **impose friction** to, in the short term, directly disrupt adversary operations;
7. In the medium term, friction will ***reduce an adversary's ability* to attack**;
8. There will also be a stabilizing process of **tacit bargaining** between adversaries as they mutually discover the upper and lower bounds of conflict through repeated interactions;
9. US cyber forces will simultaneously use more purely offensive cyber capabilities for **deterrence** purposes, reducing an adversary's *willingness* to attack;

Result

10. Adversaries will, over the long term, moderate their behavior in response to US actions, creating a more **stable environment and continued U.S superiority**.

Even hawks acknowledge that **some crises have no military solution**. If persistent engagement leads to positive feedback, the United States may have to accept that this is one of those situations. Persistent engagement could also fail if the United States, as a technology-dependent democracy, is unable to play the game hard enough to win. In either case, the US may only be able to realistically establish stability through defense or non-cyber responses or by forgoing the goal of cyber superiority or "overmatch."

The Way Ahead:

1. Future US policies and strategies, as well as academic research, should not be based only in a select subset of dynamics, but rather examine all the major themes: speed and agility, universal vulnerability, uncertainty, perceived lack of restraint, covert usability leads to persistent engagement, outsized role of non-state actors, and early use leads to surprise attack.
2. Persistent engagement will place military and intelligence forces in close contact, actively contending with each other. If this dynamic isn't to spiral out of control, there must be military-to-military hotlines and other mechanisms to reduce the chances of miscalculation.
3. "Forward defense" must be conducted as an experiment, with clear criteria for failure and success. The US must be open to the evidence and change course as necessary.
4. SIPA, with the Cyber Threat Alliance, is developing an analytical framework to help assess if adversaries are increasing the number, recklessness, or aggression of their attacks. This can suggest if an offensive deterrence posture is working as intended or failing and introducing positive feedback.
5. Persistent engagement in cyberspace represents perhaps a radically new kind of conflict which demands significant new study, not just on how to prevail, but coercion, deterrence and escalation; and the changing nature of civil-military relations.