SYNESIS
A JOURNAL OF SCIENCE, TECHNOLOGY, ETHICS, AND POLICY

# International Systems, Polarity, Cybertechnology and Stability

Felix Willem Huesken[1]

1. New College, University of Oxford, Oxford, UK, OX1 3BN, E-mail: fwhuesken@gmail.com.

***Abstract***

*Stability in the international system is the key to security. This paper will discuss the four possible distributions of power – multipolarity, bipolarity, unipolarity, nonpolarity, - and explain why the stability that each distribution provides is decreasing in the order given. Bipolarity was more stable than multipolarity. However, cybertechnology may destabilize a bipolar order. Cybertechnology influences stability in various ways. In a cyber-based environment, advantages lie with the attacker: stealth, anonymity and unpredictability, and this poses incentives to strike preemptively. Cyberwarfare is also economically cheap; all that may be needed are talented hackers, intelligence on target, and viable computer and network connections. Hence it is also an easy way to amass credible force and wield power. The virus Stuxnet showed that simply cutting an internet connection or establishing computer systems that are not connected to any others in a local area network does not prevent assets from being assailed. False-flag operations to trick a third state into attacking one's enemy are frighteningly easy. Thus, it is argued herein that multipolarity is the only scenario in which cybertechnology might mitigate forces leading to instability.*

*Keywords: International systems, stability, cybertechnology, multipolarity, cyberwarfare, deterrence*

*"In the 21st century, bits and bytes can be as destructive as bullets and bombs"*

*— William Lynn,*
*United States Deputy Defense Secretary*

In this essay I will distinguish the four possible distributions of power in the international system — multipolarity, bipolarity, nonpolarity, and unipolarity — and explain why the stability that each provides is decreasing in accordance with the order above.

After providing a definition of stability, the essay will turn to each power theory in detail. It will discuss how cybertechnology can change the stability of the international system. Through both current and historic examples, the final section will attempt to show why the aforementioned ranking is justified. It will also posit how cybertechnology has already fundamentally threatened stability in the previously bipolar setting, and will conclude by arguing the potential stability benefits that may be facilitated by multipolarity.

## *Stability*

Two definitions of stability, one narrow and one broad, are important to note. Mearsheimer defines stability in the international system as the absence of war and ma-

jor crises (1). He focuses narrowly on the third image analysis. Deutsch and Singer take the broader approach and take both 2nd and 3rd image into account (2). Accordingly, stability can be considered from two points of view: from the perspective of both the total system and the individual state. From a systemic vantage point, this differentiates Mearsheimer's definition only slightly. Stability at the nation-state level is defined as the probability of the state's continued political independence and territory in conjunction with the non-probability of becoming engaged in a war of survival (2).

### *Bipolarity*

John Mearsheimer claims that bipolarity is a more peaceful arrangement of power and sets out three characteristics. All three can be referred to as being divisive; what makes bipolarity more stable is that these characteristics occur less frequently than in a multipolar system. First, with only two main power centers, the number of conflict-generating dyads is smaller and makes war less possible. Minor powers have difficulties sustaining a position of neutrality when major powers often demand allegiance. Furthermore, with only two major powers, minor states have fewer opportunities to barter such power dyads off each other. In general, a bipolar system is much more rigid in terms of the possibilities and opportunities available to both major and minor powers.

Second, since there are only two major powers, deterrence becomes easier. With minor powers either being attached to one of the two major powers, or being too small to influence the system, imbalances of power occur less often (1). Van Evera's framework of offense-defense dominance establishes that the defense dominates if the so-called first-move dividend is too small to shift the force ratio in the attacker's favor (3). Deterrence is most likely to be effective when the costs and risks of war are great (1). As Mearsheimer points out, this may not hold to the same extent with conventional warfare as it holds with nuclear warfare (1), wherein preemptive wars have less attraction; initial aggressors can be checked and defenders can succeed even if they lose the initiative (3). Nikita Khrushchev provided an insightful example of this idea during the 1962 Cuban Crisis when he remarked that Soviet missiles stationed in Cuba were "defensive weapons" (3).

Third, if states decide to deter, the prospects of such actions tend toward being more positive. With only one opponent, the other state will find it easier to calculate the relative power and the opponent's determinations (1). However, classic deterrence does not always function in the same ways when considering the power dynamics of bio — and cybertechnology.

Mearsheimer does not specifically consider other weapons of mass destruction such chemical and biological weapons. Mearsheimer's reasoning not to include such weapons is that there are fundamental differences in the possible military use of those weapons. Their impact radius, impact time and future consequences are hard to estimate and control. Except for fallout, nuclear bombs can be considered as simply very large bombs, and thus fit in the framework of experiences that militaries have acquired over the past century. Biological and chemical weapons may well be used for terrorist attacks, but, with the exception of state-sponsored terrorism, a discussion of such forms of terrorism would be beyond the scope of this essay.

From the end of WWII until the 1980s — the time period Mearsheimer is concerned with — the principal threat of biological weapons stemmed from state-run programs. Fortunately, such agents were never unleashed on a large scale (4). As of March 2011, 164 countries (including unofficially, the Republic of Taiwan) have signed the international Biological Weapons Convention (BWC). The BWC outlaws acquiring, possessing, developing, and proliferating biological weapons; states must destroy or divert to peaceful purposes all existing biological weapons prior to signatory participation (5). Note that the BWC does not make unlawful the use of biological weapons, as this has already been addressed by and proscribed in the Geneva Protocol of 1925 (6).

The status of chemical weapons is similar; their use was ruled to be illegal by the Geneva Protocol in 1925 (6), and chemical weapons were eventually outlawed in 1992 by the Chemical Weapons Convention (CWC) that has now been signed by 188 countries worldwide (7).

Both biological and chemical weapons are now illegal to use, develop, possess, proliferate etc. in most of the countries in the world. For the sake of argument let us assume that this is sufficient to prevent any state from using such weapons[i]. However, that does not prevent non-state actors, e.g., terrorist groups, from trying to acquire or develop those weapons. The impact of a terrorist attack with biological and/or chemical weapons on the stability of the international system is hard to estimate. It is unlikely that

it would have the same impact as a large scale state attack. Terrorism, by its very nature, does not conform to discrete state boundaries. Therefore, it would be difficult for any state that incurred such an attack to retaliate in similar or equivalent manner.

As already noted above, an advantage of bipolarity is that power imbalances are largely absent; if they do occur they are countered quite efficiently by either internal or external means. Neither of the two actors has an opportunity to conjoin with fellow major nations to manipulate its opponent. In general, power imbalances resulting from such conjoinment (and national bullying) represent endogenous shocks to the system, and are not probable or sustainable within a bipolar system (1).

If exogenous events shock the system and power imbalances develop, the required balancing[ii] by external and internal means can be achieved quickly and efficiently. By external means, balance may be gained through diplomacy and alliances. Both of these tools of international politics are more prone to be used in a multipolar world, however. States quickly change from one alliance to another or use diplomatic means, such as embargos, to influence the balancing process (2). Through internal means, balance is achieved by military buildup. These means are directly under state control. Therefore, they tend to be more efficient and more certain to produce real balance (1).

Yet, the claim that internal balancing is more efficient can be argued against supporters of bipolarity. Since this mechanism is used almost exclusively in a bipolar system supporters claim that is also a more stable approach. Internal balancing equates to arms build-up. Increasing military power, even if intended for purely defensive reasons, may provoke even stronger reactions by the opposing state, and ultimately lead to exponential growth of military power (2). Such an arms race is dangerous for two reasons. First, it opens windows of opportunity and vulnerability, and may encourage a state to preemptively strike when one side is in the lead (3). Second, the rapid military change fosters false optimism and may confuse political estimates of relative power (3). In general the problem is one of false perceptions. States either underestimate the military power of the opposing side, or overestimate their own military power and/or the number of perceived allies (1). For these reasons, arms races are to be avoided. In general, countries tend to be more likely to react to increases in military power of rivals if it is reasonable that they might be directed and deployed against themselves. In a bipolar environment, this distinction does not exist. There is only one rival and all changes in military are necessarily directed against the opposing state. Thus, arms races tend to be faster under bipolar conditions than under multipolar conditions (2).

A recent example of bipolarity in the international system is the Cold War between the United States and the Soviet Union. Both parties gathered a number of allies, especially in Europe. A number of proxy conflicts ensued, e.g. the Vietnam War and the Cuban Missile Crisis of 1962 was precipitously close to causing a nuclear showdown. However, for most of the Cold War, deterrence via mutual assured destruction worked fairly well (1). Despite proxy wars, the US and the USSR fought for economic preponderance instead of direct confrontation by military means, and this was often symbolized by propaganda related to iconic endeavors like the "race to the moon".

### *Multipolarity*

Deutsch and Singer present three arguments to show why multipolarity may be a more stable arrangement. First, the greater the actors in the international system, the more interaction opportunities and the more relationships between states become possible (2). Two phenomena result from an increased number of actors: negative feedback and cross-pressuring.

Negative feedback is a form of self-correction — stimuli and effects in one direction are offset by forces that initially weaken the response to these stimuli and later increasingly countervail it. The system thus restrains itself; it is contrary to a self-reinforcing system (such as the recent housing-price bubble) (2).

Cross-pressuring is based on the state's different attitudes towards international issues. In general, states will coalesce with other states depending on the issues at hand. A relatively large number of actors and the parallel greater interaction opportunities produce a set of cross-pressures that largely inhibit any superimposition or reinforcement of states' positions on different topics. In the end, common interests are established (2). The process is similar to Adam Smith's "invisible hand" determining market prices (8).

Second, with increased numbers of independent actors, the share of attention each country can devote to others necessarily diminishes. This is not to say that each actor

gets an equal share of a state's attention. The attention capacities[iii] of each state are allocated in ways that assign greater weight to relationships in which it is a partner versus those relationships in which it is not a partner[iv]. This can counter the claims advanced by supporters of bipolarity that a greater number of relevant actors in a system increases the likeliness of conflicts (1). To the contrary, the counterargument's premise is that interaction between states is a special case of exchanging messages. Communication theory explains that after a certain threshold, signals turn into noise from which particular messages cannot be perceived. Similarly, a government would devote most of its attention to its most imminent adversary and regard other messages as noise, relevant to any current conflicts (2). To engage in conflict a government requires a focused attention ratio[v]; lest true adversaries would not be recognized as such (2). Therefore, with an increased number of independent actors, the share of attention each nation can devote to particular actors diminishes, and the system as a whole becomes inherently more stable (2).

Third, most balancing in a multipolar system is external in nature. It will produce a distribution of power among evenly matched coalitions, as long as most powers are free to move from one coalition or alliance to another. Thus, in contrast to bipolarity, arms increases by a rival power might be solved by quick rearrangement of alignments instead of arms escalation (2).

However, the agile changing of alliances by actors in the international system after with a conflict also induces a number of serious coordination problems. Alliances face problems of collective action. Being a member in an alliance is consumption of a collective good. In the case of crisis, members may be tempted to refrain from engaging on the part of an ally, and "buck-pass" alliance burdens. This is most likely if the number of states that form a blocking coalition is large (1). A state may also consciously opt to stay on the sidelines when facing two potential rivals. A war between two rivals might improve a third state's power position relative to both combatants (1). States may somewhat riskily decide to opt out of the balancing process because they simply believe not to be targeted by the aggressor. Diplomacy is certainly a viable option, but remains a process of uncertainty and unintended outcomes. It takes time to build a defensive coalition. An aggressor might reason that any coalition-building will be too slow to prevent an attack (1). Conquest is now easy and moving first is viewed as more rewarding (3); the balancing process becomes slower and even further destabilized. For these reasons, states might become disenfranchised in balancing efforts and might then have incentive to bandwagon with the aggressor, leading to additional system destabilization (1).

An example of multipolarity in the international system can be seen in pre-World War I Europe. Five powers — Germany, Austria-Hungary, France, Russia and the United Kingdom — were deeply connected in a web of alliance treaties and partially secret agreements, at first woven by Chancellor Bismarck of Germany. However, in 1914 two alliance systems were established: the Dual Alliance (Germany, Austria-Hungary) and the Triple Entente (France, UK, Russia). This alliance system was a source of security. Through a constant realigning with each other, the participants had been struggling to assume positions that would allow the greatest degree of security. At the time of the assassination of Austria's Archduke Ferdinand, European power politics had become a two actor, zero-sum game. The states became concerned with relative power gains, and the notion that mutual mobilization meant war became a self-fulfilling prophecy (9).

At this point, a note about alliances seems worthwhile. In general, alliances both ensure stability and trigger conflict. They are presumed to provide stability by easing the resolution of conflicts short of war, and restricting the scope of conflicts that do occur (10). However there seems to be a threshold for which alliances can sustain these effects, the critical factor being the size of the alliance members. Sabrosky notes that prolonged alliance building around the same contending major power centers (as before World War I) as well as no clear pattern of alliances (as preceded World War II) often has devastating effects. Under these circumstances the system can become both more crisis-prone and more war prone (10). Deutsch and Singer argue similarly — a state in alliance minimizes the range of issues and the intensity with which it might initiate or engage conflict with fellow alliance members. On the other hand, such a categorical insider-outsider division can lead to an accretion in the range and intensity of conflicts with non-alliance actors (2).

### *Unipolarity*

Unipolarity is also known as hegemonic stability; based upon economic and military power, a hegemon provides leadership and ensures stability in the international system. By setting rules for economic transactions, it secures

investments abroad. Other powers benefit from the status quo, but not to the extent as the hegemon. At the same time, the hegemon serves as the steward, the persecutor, and the greatest beneficiary of the unipolar system (11).

The most recent example of unipolarity is the United States after the Cold War. The relative bipolar system in place since the end of WWII was shattered by the collapse of the Soviet Union. Today, the United States is without rival in any of the standard components of power. Its military advantage has been both quantitative and qualitative, spending more on military research and development (R&D) than major European powers spend on defense in total (12). Despite recent financial crises, it remains the leading economic power in the world (12) This dominance in the military and economic realms is rooted in technological capabilities, investing more in research and development (R&D) than the next seven richest countries combined (12). Brooks and Wolfforth express the uniqueness of the current US position in the international system by stating "…if today's American primacy does not constitute unipolarity, nothing ever will" (12).

However, the stability of the international system under continued US primacy is a topic of some dispute. In general terms, the exposed position of the hegemon is also the most dangerous. Growth of power is uneven; it can occur due to changes in transportation, communication, technology, population, or economic and military capabilities. The cost-benefit ratio of being the hegemon can also be contributory to the decline of the hegemon. Since it is the most benefiting actor, the hegemon is also most interested in maintaining the status quo. Therefore, it must put more effort into the system than other states, and must also deter possible challengers. The short-run rewards of hegemony can also lead to a tendency for overemphasizing consumption at the expense of investment (11). With declining relative growth rates, the power base of the hegemon erodes and power shifts away to other states (11).

Thus, there are two ways in which this system might fail as the hegemon is trapped in the declining relative power it can exercise. First, challengers see a window of opportunity (3) and initiate war to expand the limits of their newly acquired power capabilities (11); second, the hegemon might recognize its declining power and attack possible challengers in order to check their advancements and threat (11). There is a greater incentive to strike preemptively, if and when moving first is more rewarding (3). With time the hegemon's effort to maintain the status quo increasingly becomes more difficult, and conflict-based strategy is more likely to be applied.

### *Nonpolarity*

Nonpolarity represents a world characterized by numerous centers of meaningful power[vi]. Power is diffuse; sovereign nation-states are not the only kind of power actor, and are instead under pressure from militias, challenged by non-governmental organizations (NGOs) and multinational corporations (MNCs), by regional and global commercial organizations (13). Power, rather than being concentrated, is distributed among and between actors of nation-states, global media outlets, large scale economic commerial entities, religious groups, terrorist groups and drug cartels, NGOs and MNCs, global cities, diaspora political parties, and others (13).

With so many actors having significant power and asserting influence, nonpolarity, following realist thinking, increases the number of threats and vulnerabilities to each country. In the absence of external intervention, entropy dictates that systems consisting of a large number of actors tend toward disorder and greater randomness (13). As Haass has rather colloquially summarized: "… herding a dozen is harder than herding a few" (13).

If the prospects appear so negative, why could nonpolarity occur on the world stage? Haass gives three reasons for nonpolarity's rise, and the failure of powers to become strong enough to challenge US hegemony. First, nonpolarity is a function of experience. States, as well as corporations and organizations, strengthen their skills in developing and consolidating human, financial and technological resources that lead to productivity and prosperity. This process, and the accompanying aggrandizement of new powers cannot be easily stopped; thus, an ever-larger number of actors are able to exert influence at both regional and global levels (13). Second, nonpolarity is partly caused by policies adopted by the hegemon in the unipolar system it has established. For example, US reliance on foreign oil resources has led to a transfer of wealth to oil-producing countries and companies around the world. Moreover, the inflated current account deficit, and the related weakness of the US dollar have led to expansion of wealth and power elsewhere in the world (13). Third, possible challengers of US hegemony, like the CRIB (China, Russia, India, Brazil) states are as yet weak and fail to leverage internal power on a broad external scale. At the same time, Haass advances the lib-

eralist view that these powers depend on the international system for economic welfare and political stability. Thus, the resistance to play the great-power role may represent a deliberate decision by these countries — at least in part and at present (13). It is in essence a reaction to, and an inevitable consequence of globalization[vii]. This reinforces nonpolarity by prompting power development outside the control of governments (and are thus not initially noticed), and this strengthens the capabilities of non-state actors who can easily transfer monies, goods, ideas and human resources using the global networks readily at hand (13).

Although Haass describes the current international system in an interesting and at first convincing way, I believe that his policy recommendations for a nonpolar system are circular. Nonpolarity is caused by increased international integration, which gives rise to non-state actors and diffuses power widely across different kinds of actors. The consequences tend to be mostly negative. Haass advocates reconstituting the UN Security Council and Group of 8 to reflect changes in the international system after World War II. He identifies multilateralism as essential for the nonpolar world (13). At the same time he describes alliances and bilateral relationships as situational and short-lived. Cooperation is based on the subject; a classification of countries as allied and/or adversarial will become ever more difficult. Haass advances a greater degree of global integration[viii] to help promote stability, yet neglects the origin of nonpolarity as lying in the increase of cross-border flows and the rise of non-state actors in an ever more integrated world. Haass has developed this hypotheses only recently, and claims that in reality the current system is nonpolar. As provocative as this claim is, I feel that the actual dynamics of hegemony are overlooked. Hence, while offering a vision of a world that "could-be", Hass descriptions are best held to be a warning or the future, rather than an authentic view of the present. Still, his perspective may be of value when considering if and how current developments in science and technology might affect the near-future dynamics of the international system.

### *Technology and the international system*

Developments in science and technology have always shaped the international landscape. They enable the exploration, conquering and control of places and people. In the late 20th and early 21st century, two technologies are particularly important in their impact upon the world-scene: biotechnology and cybertechnology. Both have shaped knowledge of and in world, and human influence upon nature. Both technologies have brought significant changes to personal, public, and professional lives and the perspectives that impact international relations theory.

### *Cybertechnology*

There are various ways to define and describe cybertechnology, one reason why the implications of this science and technology remains only partially understood, and cyber defense strategies are still nascent — although are expanding rapidly in both pace and scope (see, for example, Sample TR, Swetnam MS. #CyberDoc No Borders — No Boundaries: National Doctrine for the Cyber Era, Potomac Institute Press, 2012). From the military perspective, Gen Michael Hayden, positions the cyber realm as one of five domains of political combat: (i.e., land, sea, air, space and cyber), and as such, is the first domain to be created by man (14). The so-called "cyber cake" consists of three layers: the bottom is the physical layer; the middle is the syntactic layer, and the icing is the semantic layer (15). The physical layer consists of computational devices and connections between them i.e., wires, signals and/or other means. If the physical layer is disrupted the system as such, can also be disrupted; a consideration of interest when cyber protection is discussed. The syntactic layer contains operating instructions of designers and users, and the protocols through which machines communicate with each other e.g., device recognition, packet framing, addressing, routing etc. The semantic layer contains all the information in the machines and the system (at a variety of scales) (15).

The cyber realm also abounds with private networks. Companies such as Google offer vital services to private users, governments and the economy, services that were privately developed, yet existed in an environment initially created by the US Department of Defense (14). To some extent, governments have lost a fair modicum of control within the cyber domain. In some ways, this can be seen analogous to the history of exploration of the Western hemisphere. Large companies, like the Hudson Bay Company and East India Tea Company, acted with many attributes of sovereignty. To date, it remains unclear to what extent Google and other such entities will expand control within the "terra nova" of cyber, and whether the profits gained should be invested in embellishing and securing their own networks. How much responsibility for the security of these vital services lies with the providers? Is it overstretching or undermining the judicial system to

allow those companies to act on their own in countering cyber attacks; a new form of letters of marque and reprisal (14)?

### *Cybertechnology: threats*

In the cyber realm, considerable advantage lies with the attacker: stealth, anonymity and unpredictability (16). The internet is the main component of the cyber environment and is designed to be collaborative, rapidly expandable, and easily adaptable to technological innovation. Information flow has taken precedence over content integrity; identity authentication less important than connectivity (17). Threats to cybersecurity can be divided into three categories: external threats, internal threats, and supply chain threats. Internal threats by rogue operators or double agents will not be discussed here; in contrast to other threats to date, they occur too rarely. External threats are more commonly known as hacking. Hacking, if defined in the most basic sense is asserting one's own authority in a system over the authority of its designers and users. Hackers speak of "owning" a machine or network. The term is misleading as most times hackers do not seek to garner attention when preparing and conducting attacks (15). Hacking tends to occur on the middle level, i.e. the syntactic layer (15). In this light, distinctions made between information on the semantic layer and instructions on the syntactic layer are misleading (15). Oftentimes, hackers use tools that appear to be information, such as compromised attachments or websites with embedded code. These tools work very much like tricking a thermostat into chilling a room by holding a match beneath it — that is, by providing false inputs and information. However, most network systems do not accept false information unless changes have been implemented on the the syntactic level, as well (15).

Supply chain threats develop when hardware and software components are changed before they are integrated into a designated system. This is possible at all stages of the production process: design, manufacturing, service and distribution. Even unwarily disposed components can provide information required to infiltrate an operational system (17). Most times, supply chain attacks are accomplished using so-called trojans, small programs hidden in equipment circuitry activated either by a signal from outside, or when the tampered system is in a certain status (e.g. when a usually passive radar system enters into active search mode) (18).

How does the cyber domain change the stability of the international system? Does this new domain create opportunity for more conflicts and hence more instability? Or is it merely another — albeit a new and complex — theater in which possible attackers can be identified and deterred?

### *Cybertechnology: attacks*

There are two types of infiltrations: cyber network espionage (CNE) and cyber network attacks (CNA). The differences between the two may seem marginal at first, but are in fact meaningful. CNE is spying using computer networks; it causes consequential harm by having secrets stolen (15), and is a technique that most nations, if possessing the capabilities, engage in (19). Although espionage is rarely considered an overt act of war, it is difficult to sufficiently determine whether a malicious program found in a network has been installed for the purpose of spying on current data being processed, or to induce disruptive harm(s) at a later time (17), e.g., as was allegedly used by the Israeli Air Force in 2007 to disable Syrian radar during an attack on a nuclear facility construction site (18).

CNA is disruption and corruption of other networks. Whereas the Israeli use of cyberwarfare can be regarded only as a tactical measure in an otherwise conventional attack, three years later, an as yet unknown attacker infiltrated computational networks(s) of Iranian nuclear facilities. The virus used was called Stuxnet, the first-known virus specifically designed to target cyber infrastructure (20). It was not spread via the internet, but by small USB flash drives; once installed in the system it covertly self-replicated and spread, opportunistically exploiting vulnerability in the LAN system until it was introduced to the main target computer (21). This computer controlled the uranium enrichment centrifuges; thus, the virus disrupted the Iranian nuclear program, the most probable goal of the attack (20). This attack was seen as crossing the proverbial Rubicon into the age of cyber conflict[ix], due to its sophistication, specification, and costs (22). Given such incurred costs, it is also likely that the virus was developed by a state or was at least state-sponsored. This was not the first instance of accusations of state-sponsored cyber-engagement. For example, during a state visit to China in 2007, German Chancellor Angela Merkel accused the Chinese government of hacking into a number of German government networks. Security officials believed that the hackers were guided by the People's Liberation Army,

and that the programs were redirected via South Korea to disguise their origin (23).

Another threat to cyberspace is kinetic energy. Destroying the physical foundation of computer networks can be done by damaging server hubs; a rather old-school method that resembles the specific targeting of telegraph poles during World War II. At present, China remains exceedingly vulnerable in this regard. For purposes of state-monitoring, all internet traffic is routed through Beijing, Shanghai, and Guangzhou (15). Simply destroying these access points could sever China's internet access, and disrupt the intra-Chinese computer networks communications.

### *Cybertechnology: the attribution problem*

Rather colloquially, in the cyber battlespace, we do not know who shot, do not know from where we were shot, and we do not know what is going to happen next. Attribution is the fundamental problem of cyberspace, and this is important, with regard to retaliation. In the cyber realm, when an attack cannot be assuredly attributed the question is raised: if attribution is difficult, if not impossible, why remain innocent (15)? Correct attribution is obviously important to justify retaliation. In contrast to the Cold War, third parties have developed significant cyberattack capabilities. They need to be convinced that the retaliating state was really attacked and that the retaliation is aimed at the correct country (15). Otherwise, retaliation might be regarded as unjustified, and resulting sanctions could range from loss of international reputation, to economic restriction, to war.

Although seemingly odd, the attacking state must also be convinced that attribution is correct. Most of the time the attacker it is aware of the attack. However, the attacking party must be convinced that any retaliation is directly due to the targeted entity's knowledge that it was attacked, and this attack seeming as the basis for action. Cyberspace poses the problem that many attackers can operate at once, and with independence (15). This situation is hardly imaginable for conventional, let alone nuclear war.

Why is it so hard to determine the source of attack? In the main, it is because computers do not leave distinct physical evidence. In the future there might exist means and tools to search for the cyber equivalent of DNA; however at present, cyber forensic evidence remains indefinitive (15). The world contains millions of nearly identical machines capable of sending nearly identical packages (15). Rogue packets cannot be traced, instead, they are sent through multiple machines to a target; each time their originating address could be substituted by a bot that erases the packet's address and substitutes it with its own (15).

### *Cybertechnology: deterrence*

As a concept, deterrence is fairly straightforward. The lower the odds of getting caught, the higher the penalty required to convince potential attackers that what might be achieved is not worth the cost (15). Given the vast numbers of possible attackers and attack scenarios, cyber deterrence is difficult. Threats to a nation's cybersecurity range from individual hackers to organized criminal groups, from terrorist organizations to advanced nation states (24). All may have different motives and incentives. The resulting number of possible scenarios is vast: theft or exploitation of data; disruption or denial of service or access affecting the availability of networks; and destructive action including corruption, manipulation or possible degradation or destruction of networks (17). How can a suitable, effective and deterring defense be developed and maintained?

The philosophy of technology holds that there are two types of inventions; those that are made using pre-existing technology, and those that create a new technology that had not existed before. Cyberspace and the underlying technology of connecting universal computers is an example of the latter (25). According to Thomas Kuhn, revolutions in science and technology require a new paradigm, i.e., a set of laws and governing principles that replaces a now outdated, previous paradigm (25). Cybersecurity strategists seek such a new paradigm. With some merits, there have bene comparisons of the new cyber capabilities to the strategies that had been developed during the Cold War with regard to nuclear warfare. But cyber science and technology are new and rapidly expanding fields, and the potential for misjudging parameters of safety and security is therefore contingently high. As with nuclear surety and security, getting it right will be an exercise in evolution.

For the sake of argument, let us pose a case in which we assume certainty of 1) who attacked, 2) that the attacker recognizes that this is known, and 3) that we can convince third parties that retaliation is justified — in short, a legal, retaliatory cyber attack is about to begin. But can the attacker's assets be held at risk (15)? Unlike conventional or even nuclear retaliatory attacks, cyber retaliation is

usually unable to disarm the attacker. Remember, all that is needed for a cyber attack are a few talented hackers, intelligence about the target, some kind of computer and a network connection (15). What is retaliation in kind (supposed) to look like? Deterrence without credible retaliation is worth little.

### *The impact of technology*

How then can cyber checks and balances be maintained, and how migh cyber science and technology influence the nature of international systems? I offer that cybertechnology influences the international system in four ways and domains.

First, cybertechnology is closely tied to globalization, it enables rapid communication and forges connections around the world. In this environment, there is no singular opinion leader. Non-state actors can easily transfer monies, goods, and ideas. Nonpolarity becomes an even more unstable situation, augmented by the capabilities of cybertechnology.

Second, cybertechnology is cheap, so cheap that a single hacker can evoke the destructiveness of a large-scale assault upon the function of national infrastructures. It gives small states and non-state actors incentives to strike preemptively. This is especially true when striking a unipolar system; thus it becomes an uphill battle for the hegemon to prevail over time. However, these threats can be countered by the fiscal and science and technology power of the hegemon to develop and use novel cybertechnology to dampen possible challengers at an early stage.

Third, cybertechnology increases the availability and amount of information. Social media, like Facebook, Google +, Twitter etc. vastly increases the number of links between individuals and groups, and functions as a focal lens.

States encounter problems monitoring adversaries as more information needs to be processed to afford an accurate profile of current situations. Social media are distracting. In the international system, social media can stretch the attentional capabilities of states, and fewer potential adversaries reach the minimum attention ratio (2). This is especially important in a multipolar system. Here, cybertechnology may lower the risk of conflict and increase the stability of the international system (barring, of course, conflict evoked by acting upon false-positive identification of, and retaliation against perceived threat and/or attack).

Finally, given that defense against cyber attacks is difficult to establish, while a cyber offense is relatively easy to engage, cybertechnology can be seen as a dangerous element of the weaponry build-up that is characteristic of a bipolar system. Even if one great power lags far behind the other, cybertechnology can offer a cheap way to affect significant parts of the other country's populus, infrastructure, and/or economy. Cyber capabilities are also hard to quantify. As a rule of thumb, a country that spends more on science and technology research and development is likely to lead in areas of national security and defense (26). At present, that is the United States. However, if the international system becomes more bipolar, cyber capability is likely to lead to less stability.

Two additional, and dangerous phenomena of cyberspace should also be mentioned. The Stuxnet event showed that simply severing the internet connection or setting up a computer that is not connected to any other computers in a local area network does not prevent assets from being purloined (22); networks may already have been compromised. Furthermore, staging false-flag operations is easy in cyberspace. The risk of false-flag attacks grows proportionally with the threat of retaliation (15). Instead of attacking its enemy directly, the attacker stages a false-flag attack and hopes that the attacked state is fooled and retaliates — the proxy war of the 21st century.

### *Which system is more stable?*

At the beginning of this essay, stability was defined in two ways, one narrow and one broad. In ranking system theories in order of stability, nonpolarity would be lost. According to Haass, its relatively free-for-all approach has alarming consequences: it is unlikely that with so many different powers, conflict would be probable; hence the narrow definition of stability does not hold. Furthermore, smaller powers could challenge nation-states on all levels of power. It is unlikely that a state would retain all of its characteristics, and as such this fails to fulfill the requirements of the broader definition of stability, as well.

Unipolarity provides some short-term stability, but this is bound to deteriorate, for the aforementioned reasons. Namely, unipolarity provides stability in the sense that the power state will retain most of its characteristics. However, conflict will determine the ultimate stability of

unipolarity. Hegemons are limited by circumstance and time.

It is difficult to determine whether multipolarity or bipolarity is more stable. Under both systems, states are not challenged by non-state actors, as such smaller entities do not possess significant power (in contrast to nonpolarity). Multipolarity has the general advantage of more actors fortifying the stabilizing systemic effects of negative feedback, cross-pressuring and/or diminished attention. With these factors, external balancing provides an easy way to check the advancements of actors that attempt to increase their sphere of influence. Bipolarity, in this scenario, can react to changing power distributions only by internal balancing, which is prone to result in races of resources, economics, and weapons.

Nevertheless, Mearsheimer's claim that bipolarity offer "…simplicity, breeds certainty; certainty bolsters peace" (1) may be in many ways correct: a reduced number of actors leads to greater stability if the preceding system was nonpolar. In contrast, too great reduction can be harmful, if the resulting system becomes unipolar. Whether the most stable system is one of only two actors, or more than two, becomes debatable. Reality most probably lies somewhere in between. Given results of the latest episode of multipolarity, World War I, it may have been tempting to crown bipolarity as the most stable distribution of power, especially since the stand-off between the US and the Soviet Union ended peacefully. However today, given the capabilities of cybertechnology, only a multipolar system might be viably stable, only if, and only if, we learn to operate safely in an already compromised environment; and only if we improve identification mechanisms to impair false-flag attacks.

## *Conclusion*

The preceding discussion may be little more than an academic exercise. We live in the system that is given to us, not by some over-arching power but by the actions of human societies themselves. We may discuss which system would be more favorable for humankind, and may all agree that it is multipolarity (or some other construct). Yet, there is no way in which we can form alliances and integrate states and challenge the greatest powers. And there is no way in which we can agree on which players out of many should or shall be our power centers. Systems are initiated and ended not by close assessment of the interests of the state at every given moment, but by cataclysmic external events. The structure of the international system does not move in phase with changes in the distribution of power (27). In essence, states are path-dependent. They adjust to shifts in the international system by developing and installing institutions to contain new environments (27). These institutions tend to be "sticky", and remain in place long after their existence exerts positive effects and could be justified. Whether change occurs in terms of technology, transportation, communication, population, economic and/or military capabilities (11), it often takes unanticipated courses (28) and can exert unintended consequences. On the current world-stage, change is often caused and catalyzed by technology (11,28). Technology can both unify and estrange us on individual, community, national, and systems' levels. By definition, technology is intended to make private, professional and social life easier. It also changes life fundamentally, and in so doing can fundamentally that it changes the nature of the international system. A system, in existence for centuries That has been the basis, forum and result of our wars and peace. It remains to be seen how we — as agents, actors, states, and a global pluralist culture — will develop and employ cyberscience and technology to influence, shape — and be affected by — the balances of power within international systems.

## *Competing Interests*

The author declares that he has no competing interests.

## *Notes*

i. Note that the last chemical attack conducted by a state was on March 16, 1988 by Iraq under the regime of Saddam Hussein; the attack is also known as the Halabja poison gas massacre. Iraq signed but not ratified the CWC in 2009.

ii. Change of concept of "balance of power"; now used meaning "policy recommendation" (see 1).

iii. Defined as a nation's total information-processing and resource allocating capabilities.

iv. The relationships in which a state is not a partner but which receive some degree of attention are typically the relationships between the state of concern and its allies.

v. Defined as attention to messages from rivals to attention from messages from all other states.

vi. The definition provides the missing piece in the different possible power distributions of the international system — three or more distinct poles as in multipolarity, concentrations of power revolving around two opposing positions as in bipolarity, and domination by a single power as in unipolarity.

vii. Globalization defined as the increase in volume, velocity and hence importance of cross-border flows.

viii. Advances in particular the idea of "concerted nonpolarity", a core group of governments and other cooperative organizations, which would manage the international system.

ix. Cybered conflict differs from cyber war or cyber battle. The latter is fully technological and could, in principle, be conducted entirely within a network. It is normally a component of the former. A cybered conflict is any conflict of significance of national significance in which key events determining the path to the generally accepted outcome of the conflict could not have proceeded unless cyber means were nonsubtitutable and critically involved.

### *References*


1. Mearsheimer JJ. Back to the future: Instability in Europe after the Cold War. In: Brown ME, Coté OR, Lynn-Jones SM, Miller SE, editors. Theories of War and Peace. Cambridge, MA: MIT Press, 1998. p. 3-55.
2. Deutsch K, Singer JD. Multipolar power systems and international stability. World Politics. 1964 Apr;16:390-40.
3. Van Evera S. Offense, defense, and the causes of war. In: Brown ME, Coté OR, Lynn-Jones SM, Miller SE, editors. Theories of War and Peace. Cambridge, MA: MIT Press, 1998. p. 55-94.
4. United States National Security Council. National Strategy for Countering Biological Threats. 2009.
5. United Nations Office at Geneva [Internet]. Disarmarment: The Biological Weapons Convention. 2011. July 4. Available at: http://www.unog.ch/80256EE600585943/%28httpPages%29/04FBBDD6315AC720C1257180004B1B2F?OpenDocument.
6. The Biological and Toxin Weapons Convention Database [Internet]. Text of the Biological and Toxin Weapons Convention Database. 2011. July 4. Available at: http://www.brad.ac.uk/acad/sbtwc/keytext/genprot.htm.
7. Organization for the Prohibition of Chemical Weapons [Internet]. About the OPCW. 2011. July 4. Available at: http://www.opcw.org/about-opcw/.
8. Smith A. The wealth of nations. London: Penguin Classics; 2000.
9. Waltz K. Man, the state and war: A theoretical analysis. New York City, NY: Columbia University Press; 2001.
10. Sabrosky AN. From Bosnia to Sarajevo: A comparative discussion of interstate crises. Journal of Conflict Resolution. 1975; Mar;19:3-24
11. Kohout, F. Cyclical, Hegemonic, and Pluralistic Theories of International Politics: Some Comparative Reflections on War Causation. International Political Science Review: Power Cycle Theory and Global Politics. 2003 Jan;24(1):51-66.
12. Brooks SG, Wohlforth WC. American Primacy in Perspective. Foreign Affairs. 2002 Jul-Aug;81(4):20-33.
13. Haass RN. The age of nonpolarity: What will follow U.S. dominance? Foreign Affairs. 2008 May-Jun;87(3).
14. Hayden M. The future of things "cyber". Strategic Studies Quarterly. 2011;5(1):3-7.
15. Libicki MC. Cyberdeterrence and cyberwar. RAND Corporation; 2009.
16. Markoff J, Sanger D, Shanker T. Cyberwar: In digital combat, U.S. finds no easy deterrent. New York Times. 2010 Jan 26.
17. Department of Defense. Strategy for operating in cyberspace. 2011.
18. Markoff J. Old trick threatens the newest weapons. New York Times. 2009 Oct 27.
19. Wilson C. Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congress. Congressional Research Service. 2008 Jan 29.
20. Fildes J. Stuxnet virus targets and spread revealed. BBC News. 2011 Feb 15. Available at: http://www.bbc.co.uk/news/technology-12465688.
21. Falliere N, Murchu LO, Chien E. W. 32. Stuxnet Dossier. Symantec. 2011 Feb.
22. Demchak C, Dombrowski P. Rise of a cybered Westphalian age. Strategic Studies Quarterly. 2011;5(1):32-61.
23. Spiegel Online International. Espionage Report: Merkel's China Visit Marred by Hacking Allegations

[2007 Aug 28]. Available at: http://www.spiegel.de/international/world/0.1518.502169.00.html.
24. The White House. National Security Strategy. 2010.
25. Cardwell D. The Norton history of technology. London, UK: W W Norton & Co Inc.; 1995.
26. Giordano J, Forsythe C, Olds J. Neuroscience, neurotechnology and national security. The need for preparedness and an ethics of responsible acion. AJOB-Neuroscience. 1(2):1-2; 2010.
27. Krasner SD. State Power and the Structure of Foreign Trade. World Politics. 1976 Apr;16:317-347.