Blown to Bits

China's War in Cyberspace, August–September 2020

Christopher Bronk

Strategic theorists frequently lament that military planners are very effective at preparing for the last war, not the next one.[1] Planners today must cope with what conflict may look like in a new domain: cyberspace, the virtual and physical components of the global information infrastructure, what we may think of as a pre-noösphere.[2] This article projects a scenario of what a mostly, but not entirely, cyber conflict in East and Southeast Asia might look like in roughly a decade. One must hope the world's powers have learned that large-scale conventional war is an unfruitful undertaking that will disrupt our globalized international system in a manner where all lose. Of course, many of Europe's leaders believed a century ago that the menace of large-scale conventional war largely had become history.[3]

While it is the author's deepest and most sincere hope that no military conflict will come between China, Japan, India, the United States, or any other states of the Western Pacific and Asia, the massive interest in cyber conflict among these countries leads many to ponder such a struggle. We have come to recognize the Internet as a geopolitical domain for diplomacy and a potential space for conflict. In Asia, as almost nowhere else on the planet, the question of Internet sovereignty[4] is grafted onto the international system of states conceived in the time of de Groot and expanded in the crucible of hot and cold conflict during the nineteenth and twentieth centuries.

Christopher Bronk, PhD, is the Baker Institute fellow in information technology policy and a lecturer in computer science at Rice University. He also served as a career diplomat with the US State Department. Bronk earned his doctorate from the Maxwell School of Syracuse University, studied international relations at Oxford University, and received a bachelor's degree from the University of Wisconsin–Madison.

A Strategic Lens for East Asia

So what of state-centric conflict involving the Internet waged in Asia? Chinese officials sometimes speak of "our Internet," defining it not as an international cyberspace distinct of the political forces of the pre-Internet world, but rather a national infrastructure for digital communication and information dissemination. Discussion of international security in East Asia certainly considers a rising China. Boasting economic growth figures far in excess of the United States, Japan, or South Korea in the last decade and beyond, China's ascendancy has met with mixed responses in the Japanese and Korean populace.[5] Increased militarization in the region is a natural concern for both Tokyo and Seoul.[6] With Russia's place in the Far East considerably diminished since the breakup of the Soviet Union, China has begun to assert herself in a space largely filled by the United States after the Cold War.

In East Asia, the United States has, for a variety of reasons, largely engaged in bilateral security agreements, exemplified by those with Japan and South Korea. US efforts to establish a broad multilateral collective defense body in Asia on the model of NATO largely collapsed with the dissolution of the Southeast Asia Treaty Organization (SEATO) in 1977. Japan and South Korea participate, along with other US allies, in multinational military exercises and diplomatic activities, but the pair has never been tied together by formal security agreement.[7] Although Japan, South Korea, and the United States have cooperated closely on diplomacy regarding North Korea's nuclear program through the six party talks, security collaboration remains largely mediated by the United States.

In East Asia, perhaps more than anywhere else on the globe, states matter.[8] One important yardstick is defense expenditures. Where the members of the Atlantic alliance (the United States included) are pondering deep and lasting cuts in military spending, from the Straits of Malacca to the Sea of Japan, demand remains strong for sophisticated weaponry despite the attendant high price tag. Potential flashpoints in East Asia are deeply frightening. The question of the durability of American hegemony in the region is not assured, and the national politics contained by that hegemony must be considered.[9]

Admittedly, the chance of war with China still appears remote. However, the presence of tension combined with the general disinterest in moving from posturing to outright conflict may create avenues for dispute not seen previously in the international system. Asia of the 2010s will be

an interesting region because although it is economically globalized to an extremely high degree, it is also a locale where state security politics figure so prominently on the international agenda. Further, it is one of the world's most digitally connected regions, yet paradoxically one where connections are filtered by government to varying degrees. How Asia's states and peoples disagree with one another will be deeply impacted by the confluence of these realities.

Asia's Cyber (In)Security Problem

Cyberspace, which the US Department of Defense (DoD) lists as its "fifth domain" of operations (after land, sea, air, and space), is an emergent area for international dialog and potential conflict. With the cyber attacks against Estonia in 2007 and those that accompanied the use of military force in Georgia the following year, cyber operations have become more clearly connected with the scope of options available in interstate conflict. How states behave with regard to the Internet appears to matter more and more within international affairs.[10] Google's decision to direct allegations of penetrations of its computer networks by individuals in China, coupled with Secretary of State Hillary Clinton's address on Internet freedom, sent a powerful message from Silicon Valley and Washington regarding the ideals held by the United States on the governance of cyberspace. The increasingly sharp tone of communications across the Pacific on how the Internet is to be governed and policed speaks to a new soft-power politics of the digital domain that rests between government and the information and communications technology (ICT) sector.[11]

But the international politics of cyberspace in East Asia are not the sum of the two largest powers in the region. Internet conflict may be a new area of international behavior falling somewhere between diplomacy and military action. While we may not have full-blown cyberwar without war,[12] the cyber tool may be useful to governments and transnational organizations alike in voicing opinion without great cost. It may be a release valve for dissipating pressure, as may have been the case in 2001 when South Korean hackers protested the publication of a Japanese history textbook, which allegedly glossed over Japanese atrocities of the Second World War, by launching a denial-of-service attack against Japan's Ministry of Education website. There are other examples. Chinese and Taiwanese cyber activists engaged in similar tactics when cross-straits relations reached low

points in the 1990s. Also, North Korea is alleged to have launched its own computer network attacks against South Korean and US government agencies, once again knocking their websites offline with the denial-of-service tactic.

To date, the cyber attacks in East Asia have been relatively benign. Web pages are defaced, allegations of espionage are leveled, and generally a status quo of sorts is maintained. The threat politics of the cyber domain, however, do not stand still. Around the region, military resources are increasingly directed at cyber operations.[13] China, deeply impressed by US information dominance in the 1991 Gulf War, has produced a considerable literature of strategic studies for cyber operations while developing a national firewall system that shields the country from a considerable portion of web content. The United States, too, has made strategic moves in cyberspace and is in the process of building a DoD cyber command that will manage the efforts of thousands of civilian and military "cyber warriors."

Safe are assumptions that the United States' key allies in the region, chiefly Japan and Korea, will begin to collaborate more deeply on the cyber security issue. Already the head of the US Federal Communications Commission and Japan's minister of communications have indicated the need to share.[14] Indeed, a growing chorus on the international scene is considering the need for enhanced collaboration and cooperation on the detection of vulnerabilities and responses to cyber incidents. Nonetheless, there is a degree of uncertainty as to whether cyber security will be an international issue in which neorealist or neoliberal theories prevail in Asia and beyond.[15] Such uncertainty drives the scenario offered here.

Considering State Cyber Conflict—The China Scenario

This article presents a scenario of conflict[16] between the People's Republic of China (PRC) and the United States and some of its allies one decade hence. While the goal is not to get bogged down on the particulars of why such a conflict would come to pass, the real point of interest is in thinking about how cyberwar might supplant more traditional conflict and how cyber dimensions may alter warfare. To borrow from Alexander Vacca,[17] the US armed services hold different views in vying for leadership on the cyber mission. The US Navy, he argues, sees cyberspace as a contested commons, not unlike the seas, while the Air Force clings to Douhet's notions

of airpower,[18] in which opponents will pound each other's cyber infrastructure in a manner akin to strategic bombing.

Imagined here is a conflict where the *information war*, a term rightly seen as overly broad by Martin Libicki,[19] but refined to its cyber component, it is as radical a construct to conflict as airpower was in naval warfare in 1941–42. For the purposes of the scenario, I posit a conflict where China stands as the aggressor, although it is not hard to see a possible future in which China might see certain US moves as provocative and even threatening. Consider a possible future where the United States refuses to service its debt to the PRC based on human rights matters or as sour grapes over the Finlandization of Taiwan. Ponder, too, a world of the next decade where the US–India relationship continues to deepen, and the two countries warming relations and pooled sea power in the Indian Ocean leave China concerned about its access to petroleum sources and other raw materials in the Persian Gulf and Africa. Also suspend a bit of disbelief and think about a reunited Korea without US troops and a Japan increasingly driven to counterbalance China's rise with substantially increased investment in its military, particularly its navy called by another name.

Of course conflicts go from cool to hot at flash points, so for the purposes of this one, let us suppose that China, now firmly asserting itself over Taiwan as a quasi-autonomous region, faces the problems of city regions such as Shanghai, Guangzhou, and Hong Kong wishing for greater autonomy. Its large male population—a product of the one-child policy favoring birth of sons to daughters—restive and perhaps not as gainfully employed if the decades-long economic boom cools, sends Beijing looking for outside threats. The city-state of Singapore comes into focus as China's new other,[20] a sovereign entity Beijing wishes to bring inside the fold as it has Hong Kong, Macau, and Taipei. In a mostly digital rather than kinetic conflict, how might the PRC isolate the country sitting astride perhaps the globe's most important maritime choke point?

So let us imagine a late summer of 2020 in which the People's Republic of China has chosen to employ military force, largely in the cyber domain, to collapse Singapore and exert its influence monolithically over the Straits of Malacca. This is not the decision of a blindly angry dragon but rather the pragmatic move of a state needing to assert itself against a declining hegemon (the United States), a rising power (India), and an old foe (Japan) in adjusting the balance of power in East Asia.[21] With that preamble, let

us think of a war fought to conclusion, with a broader spectrum of tools, both military and economic, and with cyberwar at its heart. What follows is scenario, a sort of fiction, designed to push the boundaries of what our international system may look like in a decade. We commence with a cyberwar about to begin in a networking lab somewhere in Northern Virginia.

Laying the Field of Battle—A Clue of Cyberwar to Come

If there were any advanced warning to be had of Chinese intent, it was to be found in cyberspace. For months, intelligence analysts at the National Security Agency (NSA) and information technology (IT) managers throughout the US government handled an abnormally heavy load of probing activity on its new-generation quantum networks and legacy communication systems alike. There were numerous attempts to compromise all possible avenues to the Americans' Secret and Top Secret resources. Automated botnets consistently attempted to enter the classified computer networks of the Department of Defense, the agencies of the intelligence community, and the systems of the United States' closest allies, as had been the case for nearly two decades. Potential competitors and erstwhile allies alike read one another's mail whenever they got the chance. But in the days running up to the war, that activity spiked enormously.

Particularly alarming was a report from DISA, the Defense Information Systems Agency, in June 2020 of a piece of unknown computer code several bytes long, located as it attempted to bypass the high-to-low diode from a DoD Secret-level computer network to an unclassified host computer tracked down at an Army depot in Pennsylvania. Such an event was not at all unusual. DISA forensic specialists responded to dozens of code quarantine events of unauthorized data packets attempting to pass from unclassified to classified systems every day. Although alarms on the high-to-low passageway would occur,[22] in virtually every case the issue was some sort of false positive. Typically, there would be a software or hardware configuration error to be blamed.

Chasing down the latest high-low incident, the DoD computer emergency response team's (CERT) first-line investigators grew curious about what they had found. The small piece of data, only 256 bytes long, appeared at first glance to be senseless jumble, perhaps a broken packet piece, banging aimlessly around the network. In quarantine, it was so innocuous that the initial case manager, a mid-level civilian, had ticked the box, "Move to

dismiss" on the event report and expected the same from his subalterns. A contractor at DISA holding all-but-dissertation status in applied mathematics from Rutgers was the final name on the electronic form. Before checking himself off, the ostensibly failed number theorist decided to remove the code piece from tight quarantine and drop it onto the DISA training network. What occurred next put more than a dozen of the NSA's top mathematicians on a bus over to the nondescript DISA facility in Falls Church.

While exact details will likely be deeply classified for decades to come, assorted leaks and the information security rumor mill provide some hints as to exactly what transpired with this particular piece of unknown code. Transferred onto the disconnected training network—one which attempted to accurately simulate the convergence points of classified segmented networks and those in connection to the Internet—the code piece was observed engaging in some very peculiar behavior, in particular regarding interaction with other data on the network. It was able to reorient other pieces of code from basic applications typically found on straightforward implementations of widely used operating systems running on a variety of devices. Even more interesting was that it resisted all attempts to copy or archive it.

Watched closely, it appeared to be an intelligent software-assembling machine able to construct applications on an ad hoc basis, apparently without any outside control. Fascinating as this was to the assembled experts, even more interesting would be its sudden disappearance from the training network. After being the subject of sustained study for days, it simply vanished, never to be seen again. Some walked away from the experience claiming it to be an aberration, but to a number of DISA, DHS, and NSA participants in the forensic exercise, this odd digital artifact would do much to explain events that would come to pass in the immediate aftermath of China's commencement of electronic hostilities against the allies.

Lifting the Electronic Veil

For China, network warfare had been identified as a key area of strategic development for decades. Witnessing the stunningly lopsided defeat visited upon Iraq in the 1991 Gulf War, People's Liberation Army (PLA) strategic theorists were awestruck by the US military's incredible use of IT to direct

the conflict and bring overwhelming force to critical points on the battlefield again and again.[23] Even more, the Chinese were deeply concerned by rumors that the Americans had blinded and spoofed Iraq's high command and systematically dismantled the country's air defense system by penetrating the national information grid. That set of events, followed by the NATO operations against Serbia in the late 1990s in which American information power once again made its presence felt,[24] gave the Chinese good reason to develop their digital forces.

By 2020, the PLA had fielded an impressive digital operations command of more than 60,000 troops. Each of its seven military regions had a computer warfare regiment of more than 4,000 soldiers. In addition, a full cyber warfare division had been established outside Shanghai that was reputed to solely focus on US government and military networks. But the greatest asset held by the PRC in this area was its Information and Communications Operations Institute (ICOI), set up on a research park campus in suburban Beijing. While the operational formations in the army handled day-to-day operations and adhered to centralized tactics and operational guidelines, the ICOI was from where the big ideas on information operations emerged.

Reporting directly to the Central Military Commission but with links to the Chinese Academy of Sciences, the ICOI had at least 15,000 staff members and was essentially the national hackers lab. Little was known about the institute until the defection of a high-level employee with a PhD in artificial intelligence who had studied abroad for several years before returning to the PRC. Walking into the Australian consulate in Tokyo in July 2018, ostensibly to renew his tourist visa, the graying software engineer passed a letter to a vice-consul that would begin his journey to Canberra and eventually the United States.

While the defector was not a high-level operative of China's cyber warfare center, as those individuals were likely prohibited from engaging in overseas travel, he was the first member of its staff to find his way to the offices of a foreign intelligence service. Thorough interrogation revealed his decision to leave his home country for good came on the heels of a divorce, largely precipitated by his own deeply closeted involvement with the Falun Gong movement. The Australians were only too happy to have the defector, who they gave the pseudonym Wan Lu. After securing permanent asylum, Dr. Lu began to divulge voluminous information about his former employer.

A theoretician steeped in formal logic who toiled in machine learning, Lu offered up the major areas of attention at the ICOI. He was able to pass along the institute's reading list, which in and of itself, was an important piece of intelligence. At the outbreak of the conflict, Lu was in Canberra, where he had been set up in a research fellowship at the Australian National University, only a few miles from the US Embassy. There he stayed until the second day of the war. Certainly, the defector was of immense value to the allied cyber-warfare research community pooling on the campuses of several research universities around the United States.

Computer Krieg

Many a pundit and strategic theorist had wondered what shape unrestrained information warfare might take. The opening hours of China's virtual war with the United States and its allies over Singapore would confirm many of the worst suspicions of that crowd. Chinese forces were quite clearly working inside the decision loop of the allied forces. Preliminary moves by the PLA in the information space indicated that it could do much damage to enemy communication and computing resources, but a series of hints would reveal that China also likely had compromised, at least to a degree, the encryption mechanisms used to secure US and allied military and diplomatic communications. At times, Beijing most probably held the capacity to have a fairly complete information picture even of very high-level, classified systems, although the reverse was also likely true.

From the outset of the conflict, PLA cyber-warfare efforts were disruptive activities, highly visible to allied political and military leaders. They preceded formal hostilities, which would be marked by the sinking of a Singaporean guided missile frigate in the South China Sea on 5 September. The cyber attack had a rolling start, rather than being a bolt from the blue. When the PRC did finally choose to make use of kinetic options, the cyberwar was already well underway.

For the American and Japanese leadership, in particular, there was enormous trouble in employing even rudimentary information technologies effectively during the first days of the war. Personal computers, radio networks, satellite receivers, control systems, and battlefield communication hardware failed, often making it impossible for allied commanders to share intelligence and conduct joint planning. Only a few dedicated, high-end, satellite-based communication channels were able to connect

American field commanders in Japan and Hawaii with the Pentagon. But even these links were vulnerable, with the PLAAF's antisatellite missile attacks on 6 September producing enormous damage to US telecom satellite coverage over the Pacific.

Although Guam was the sole location of an electromagnetic strike by the Chinese, and an effective one at that, the PRC was reluctant to repeatedly use strategic missiles to short out the information grid of its enemies in the same way for fear of provoking a nuclear response from the Americans. Rather than fry the allies' systems with electromagnetic pulse (EMP) weapons, the Chinese launched attacks via the global fiber network. Often the weapon of choice was sophisticated botnets, in which legions of zombie computers and mobile devices were employed to "gang up" on unclassified government and private systems and bring them to a screeching halt in crushing denial-of-service attacks. This was especially true on Singapore, where all forms of voice and data communication, save its little-used but still operable POTS—plain old telephone service—were disrupted. Government and private networks alike collapsed in hours under withering and complex attack.

Although the Americans, Japanese, and Singaporeans had highly secure classified systems, of greater operational value to their militaries on a day-to-day basis were the general-duty, unclassified networks employed for routing supply information, passing low-level internal communications, or simply informing lower formations of their duties and responsibilities. It was at this level that the PLA displayed mastery in the operational art of cyber warfare. Although unclassified, when aggregated, the information passing across these networks provided highly useful intelligence to the Chinese on US dispositions and strategy. PLA intelligence could paint a very detailed picture of enemy movements from tracking information on cargo operations and reporting on demand for fuel and other basic supplies throughout the theater. With access to many corporate databases and networks as well, the PLA could use their information or disrupt their resources to sew chaos across the targeted countries.

Despite Google's noisy departure from (and quiet return to) China years before, many multinational corporations had unified information systems directly linked to subsidiaries in China. Those networks served as a backdoor into finance, energy, telecommunications, and defense firms alike. It took the NSA and Justice Department weeks to cut these linkages

completely, largely through isolation of all fiber-optic cables to the Chinese mainland.

Attempts to mobilize conventional forces were hampered by denial-of-service attacks against systems thought impregnable to such attack. One episode at Iwakuni, the main US Navy and Marine Corps air station in Japan, spoke to the PLA's enormous skill in knocking all manner of systems offline inside the allied militaries. Reporters from one news outlet documented it through their description of an incident on the first day of the shooting war. Hanging around with a maintenance team to research a piece on morale in the military, the American journalists scored an inside scoop on one of the biggest stories of the war. Their story painted a stark picture, which remained censored for weeks.

> Although no bombs fell on Iwakuni while we were there, the Chinese attack was felt nonetheless. [Lieutenant] Colonel Sutherland [chief operational officer for Marine Aircraft Group 12] had spent most of the morning receiving reports from the men and women who armed, fueled, and fixed the fighter aircraft on the base that their diagnostic equipment, RFID readers, and other digital tools simply were not working. The system that monitored distribution across the base had failed. Several tanker trucks had to be gotten out of mothballs just to begin getting jet fuel flowing. The devices that transferred flight plans from the planning office to the aircraft themselves all failed. Across the base, things that typically functioned for years without a hitch suddenly broke down.
>
> "Everybody's coming to me with a problem that I've never seen in my 18 years with the Corps," Sutherland was overheard to say at one point. "Nothing's working!" The frustration on the base was enormous. While Iwakuni's Marines and Sailors struggled to get their jets airworthy, reports filtered in, largely via radio, of the attack on the carrier *Carl Vinson* in the Straits of Malacca. Fearful of air raids on Japan, the pilots and mechanics put in a tremendous effort to get their planes in the sky, but that would not happen until late in the afternoon. With the loss of electronic tools, clearing each fighter for takeoff became a drawn-out manual process in which nothing seemed trustworthy at first glance.

In Washington, the president and National Security Council (NSC) were astounded at the enormous gaps in connectivity with US forces around the globe as well as the number of failed links with traditional allies in NATO and elsewhere. The vaunted White House Communications Agency, always able to connect the president with anyone, anywhere, anytime, had enormous difficulty in placing a simple phone call to the Japanese prime minister in the hour after initial reports of major cyber attack. The connectivity crisis threw into disarray contingency plans requiring key

leaders to evacuate Washington and take up positions outside the city. With communications in disarray, no one on the NSC was willing to pack up and head to Mount Weather or some other bunker dozens or hundreds of miles away. Plans for continuity of government, involving mass movements of the federal bureaucracy and leadership, were largely put on hold with only the president pro-tempore actually leaving town before dawn on the second day of the shooting war.

One line known to be functioning was the DoD hotline to Ministry of National Defense headquarters in Beijing. Several attempts to complete a call were made during the opening hours of conflict. Although nobody on the NSC knew exactly what they would say to the Chinese if they decided to pick up, there was a great sense of urgency that any and all attempts should be made in getting a dialog underway. Still in stunned disbelief, the American leadership desperately wanted to ask their Chinese counterparts, "What the hell are you doing?"

False information was also being injected into the allies' information systems. The breakdown of Pacific Command's (PACOM) logistical system underscored the level of confusion produced by the PLA's ability to place errant data at the time and place of its choosing. Supplies failed to show up where requested. The problem went beyond the military itself. Both Federal Express and UPS were forced to shut down operations for more than a week as their information systems piled up packages almost everywhere except where they belonged.

For defense planners at the Pentagon, it was hard enough to know what US forces were doing, let alone the enemy. There was good reason to believe that misinformation, mostly in the form of e-mail, was traversing allied networks. Ships at sea in the Pacific encountered all manner of navigation and datalink issues, a problem later found to involve a Trojan horse delivered to ships transiting the port at Changi, Singapore, when they hooked up to the base fiber network to perform the high-bandwidth data upload/download that was for all practical purposes impossible to do at sea via low-bandwidth satellite systems. Several warships at Pearl Harbor were found to have severe data corruption issues thanks to this Trojan, often dramatically impacting the function of their command and control systems. The carrier *Stennis*, outfitting for departure from Everett, Washington, was severely affected, but Navy officials decided to beef up her IT complement and attempt to make fixes while underway.

On Hawaii, PACOM's headquarters at Fort Shafter quickly found itself overwhelmed with data security issues. When PACOM was able to submit its initial want list to the secretary of defense and joint chiefs, it requested numbers of IT security and forensic staff outnumbering by several times the actual number on the government payroll. Heavily dependent on war rooms filled with standard commercial off-the-shelf desktop and laptop computers, staff work ground largely to a halt. No exercise at the war college could prepare the majors, commanders, captains, and colonels for the wholesale disruption of their tools. Disconnected from the DoD's global information grid, nearly all of PACOM's IT was, for several days, so much junk.

US Response

While disruptions to the American network infrastructure where visibly apparent throughout the early days of the conflict, solid estimates regarding the amount of information tapped by the PLA's network penetration activities remain hard to find. The NSA, DHS, DISA, CIA, State, the Department of Justice, and a host of other bureaus and offices pulled together every asset they had to revalidate the trustworthiness of each and every critical national security network in a manner fitting postdisaster hospital triage. There were simply not enough people to be thrown at the problem of auditing systems and taking the comprehensive measures needed to secure them for operation under the conditions of high-intensity information warfare.

Initial reports to the NSC in the opening days were bleak, with many in the cyber-intelligence and security divisions unable to see much light at the end of the tunnel. Commitment of large numbers of staff from industry and the alumni of government-sponsored information security education programs brought additional talent to the problem, but in cyberspace the PRC was dominating the struggle. Time and again, systems thought to be clean and ready for operation would begin exhibiting the same suspect behavior assumed to have been remedied. This need to revisit systems again and again drained resources and tapped expertise at a frightening pace. Many an administrator or software code auditor would spend weeks at their posts, working to answer why for every backdoor or siphon found, another would simply pop up somewhere else or reappear exactly where it had been removed before.

Answers began to come with the application of top theoretical talent from several American universities. Under the leadership of CalTech computer scientist Jules Adams, an outside working group took a broad view of the massive effort underway and began putting together ideas on the newly discovered attack techniques and patterns. For the country's brightest minds in computing, math, and a host of related fields, the challenge was to begin deciphering exactly how the PLA was employing tiny pieces of code, as located by the DISA investigators in June, so effectively. How could strings of text barely long enough to fill two lines on a piece of paper be so effective in serving as the catalyst for disrupting networks and passing data to proxy computers accessible to the Chinese?

The answer would come from a pair of digital imaging experts at the University of Rochester. Investigators had been stymied by confining their thinking on size of the malicious code at work. They were puzzled by the capacity of this data, dubbed *nanocode*, to seamlessly move from system to system, building and destroying at will, morphing, disappearing, and reappearing without rhyme or reason. Early speculation had hit on some good points, including that the code was interacting in some way with the core structures of the systems upon which it resided. But this did not explain the capacity for the malicious code sections to operate so uniquely. The New Yorkers hit on the answer when they began playing with power.

An electrical engineer by training, Prof. Goran Filipowicz first raised the question of whether the nanocode was receiving instructions facilitated by constants at the physical level. His collaborator, Tony Ikeda, a researcher on high-efficiency, low-energy imaging, had worked for years on systems that harnessed high-speed processing to construct low-bandwidth camera technology systems. He built cameras that had few pixels but took many, many pictures to create a single still image very quickly. Ikeda postulated that the nanocode was conducting this sort of framing to actually function as if it were many times larger and, even more interestingly, pass tiny amounts of data hidden in the noise of the electrical interactions on each microprocessor.

They believed the PLA had created the capacity to employ "sub-bits," pieces of noise residing in noise but able to independently communicate simple instructions and sequences. China's cyber attack, rather than an organic cellular process, was more akin to one employing sub-pieces of DNA. Bioinformaticians from the University of Washington in Seattle and the University of Toronto were the next to run with Ikeda and Filipo-

wicz's work. Operating out of a hastily constructed super lab on the campus of Carnegie Mellon University staffed with hundreds of researchers and managed by the RAND Corporation out of its Pittsburgh office, the bio-informatics team began producing evidence that the nanocode under study was obviously receiving instructions from intelligent outside sources—human beings—but also taking leads from a broad set of environmental phenomena particular to the signatures, settings, and architecture of each affected network. While the science behind the PLA's network operations was no doubt brilliant, generals at the Pentagon were not interested in discussions on orthogonality and singularity. They wanted results, especially the person at the top of the list, Air Force general Marybeth Kline, head of US Cyber Command.

Under immense pressure to get results out of the nation's computing brain trust, General Kline, a PhD in linguistics, had decamped from her headquarters at Fort Meade, which had long served as home to the NSA. Working closely with CalTech's Adams, Kline chose to spend much of her time managing the researchers, although with frequent trips back to the NSA operations center at Fort Meade. While those visits were typically immensely depressing, they kept the four star focused and on task. She would return to the revitalized rustbelt city with a new sense of urgency that was palpable to the academics, military staffers, and contractors alike. Several days after arriving and taking over the offices of the president of the University of Pittsburgh, a portrait of LTG Leslie Groves, legendary director of the Pentagon construction and the Manhattan Project, appeared on the wall over her desk. Results were needed, soon.

Progress was made, but it would be weeks before the assembled group would make important discoveries in wireless device cross-pollution and deep sleeper malicious code segments which would turn the tide in the defensive battle for control of America's cyber infrastructure. During that period, many lives would be lost due to technologies failing to function as they were intended throughout the theater of operations and beyond. Although widespread attacks on the US national critical infrastructure were few—including an incident where most of the electronic medical records of the Veterans Administration simply became irrecoverably corrupted—the PLA did not shut out the lights from Tacoma to Tampa. (The electrical grid on Singapore was crashed on the first day of attacks and stayed that way until after cessation of hostilities.)

Kline's leadership was of enormous value in overseeing the push to put systems right, but her focus on defense had not come without price. Cyber Command's attention on the defensive effort had translated to minimal activity in going after China's network infrastructure. While the Air Force's 67th Network Warfare Wing at Lackland AFB would lead the charge against the Chinese information infrastructure, it began by running stale, one-dimensional options from its playbook. Employing predictable tactics and devoid of high-level strategic input, Cyber Command's main offensive formation was also quick to reach out into academia and the private sector, commissioning every computer science graduate student in the state of Texas of US citizenship (and some not) into the National Guard by order of the governor.

Enlisting the hacker community was a job largely handled by the FBI. NSA analysts drew up a short list of freelancers, misfits, and virtuosos and passed it off to the Justice Department within days of the outbreak of hostilities. Intimidating federal agents showing up at doorsteps across the country further bolstered the ranks of the US cyber forces. Of course with the hackers, the choice was often depicted as either service or jail time. Few failed to cooperate, and although no one was actually indicted through this unusual recruiting process, stories did make the rounds of mock detention preceding a first stab at what would eventually lead to above-board, gainful employment as freelancers. Although it would take more than a month to actually string together a formal organization of this rabble, the most brilliant among this category of new public servants had an impact on the war in cyberspace almost immediately. War did not end, but rather was mitigated.

Cyberwar's Role in the Trans-Asia War

China's initial foray into cyberwar was not at all what many experts in the field had prognosticated for years. No electronic Pearl Harbor or Waterloo had occurred, and other than a few flickers here and there, the US power grid held up surprisingly well. It appears the Chinese Central Military Commission had made a calculated decision to leave much of the infrastructure up and running in the nations it had decided to wage war upon, although there is a strong counterargument that the PRC's cyber forces were largely checked in knocking out infrastructure by more than 20 years of concerted effort in building more secure systems. Whatever

the case, China's electronic forces were able to massively disrupt vital communications around the world during the opening days of the conflict. What is more, they were able to exert a persistent influence in this arena, continuing to bring down systems thought to have received a clean bill of health.

Harder to ascertain was the capacity of the PRC to draw information from the networks of the allies throughout the duration of the war. Losing trust in much of the digital infrastructure at their command, American and allied commanders often preferred to arrive at decisions by conference. Authority for decision making largely devolved to commanders in the field, many of whom believed that was how it was supposed to be anyway. Despite a long-standing dependence on IT in the execution of global command and control, US admirals and generals quickly fell back upon the initiative of their subordinates and the relationships they had developed in decades of training with foreign counterparts. Thanks to Beijing's great skill in busting and breaking into allied computer networks, there was no way for White House planners to burn the midnight oil around broad tables, sifting through intelligence and selecting targets. In the end, that was probably a net plus for the allies.

The conflict of 2020 ended with puzzling results. After inflicting considerable damage upon one another, the protagonists simply ramped back from intensive cyber operations to station keeping. Singapore retained its independence, and a naval standoff between US and Chinese carrier forces never met with conclusive end. Submarines were sunk and cruise missiles dispatched, but no bombs fell on Honolulu or Hong Kong. General war was avoided, principally thanks to a high degree of risk aversion on both sides. After approximately 55 days, the Sino-Asian conflict ended without treaty, agreement, or even much in the way of international communication.

Reflection on a Conflict that Wasn't

Although scenarios are generated, mostly by Hollywood, of a cybergeddon in which machines run amok and shadowy hackers turn society on itself, the reality is that exploitation of technological information systems, whether telegraphic taps and intercepts or radio jamming, has been a part of conflict since being incorporated into warfare. Two centuries ago Napoleon Bonaparte opined, "The battlefield is a scene of constant chaos. The winner will be the one who controls that chaos, both his own and the

enemies'." The cyber dimension, which renders all but firsthand sight to be converted into ones and zeros, will no doubt advantage those able to master it and disadvantage those who fail to do so.

For more than a decade, China's military theoreticians have pondered the role of information technology on warfare, prompted by the United States' incredible performance in the ejection of Iraqi forces from Kuwait in 1991. Doubtless, China's military officers see IT as a great leveler and force multiplier, as have Americans who spent the last decade celebrating an IT-infused revolution in military affairs.[25] In the future, whenever two relatively well-equipped and trained nation-states face off in armed conflict, the cyber dimension will no doubt be important. This article ties together some anecdotes of a war unfought by the two most powerful nations on Earth. Such epic struggles are fortunately rare in human history, but one must wonder how the Davids of our day will employ cyber weapons to bring down their Goliaths.

The major question of the scenario outlined here is: Can a forceful political objective be achieved by cyber arms alone? Perhaps not, but cyber attack certainly is a concern to those who have much to lose by digital disruption. Certainly cyber elements will be a component of future conflicts where digital infrastructure matters. To what degree malware can substitute for missiles will be decided by national governments and transnational groups in the coming years. It is clear terror organizations tend to favor real crash and bang with the attendant casualties over virtual means of inflicting damage. However, countries with much to lose by initiating kinetic actions and likely to be punished with sanctions and censure might choose the digital weapon more frequently.

In the aftermath of the Stuxnet attack, countries concerned with cyber vulnerability should prepare for the rapid mobilization of digital infrastructure remedy and repair resources. In a major cyber event, the problem set will likely be large, and the quantity of qualified talent and time available will be grossly insufficient. Steps can and should be taken in the United States to consider how to ramp up capacity for pulling together academia, industry, and government resources to meet a major contingency. Civil defense in the cyber domain must be considered a necessity.

We have not yet seen how the digital information dimension will impact conflict. While a decade ago we hoped to lift the fog of war with interneted computing, it now seems likely that new space has been created for contested perception. The digital tools for command and control have been met by

countermeasure and so on. Most likely, cyber conflict will be an "always on" engagement, even if international policy is enacted to forbid it. Sweating and bleeding will blur in this realm of conflict, as it may reside across a span of intensities from low to high. The only certainty in cyber conflict is that conflict there will not unfold in the ways we may expect. SSQ

Notes

1. John Aquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997).

2. Pierre Teilhard de Chardin, *The Phenomenon of Man* (1955; New York: Harper Perennial, 2002).

3. Michael Bordo, Alan Taylor, and Jeffrey Williamson, eds., *Globalization in Historical Perspective* (Chicago: University of Chicago Press, 2003).

4. Timothy S. Wu, "Cyberspace Sovereignty?—The Internet and the International System," *Harvard Journal of Law and Technology* 10, no. 3 (Summer 1997): 647–66.

5. "Strategic jousting between China and America: Testing the Waters," *Economist*, 29 July 2010.

6. Thomas J. Christensen, "Chinese Realpolitik: Reading Beijing's World View," *Foreign Affairs* 75, no. 5 (September/October 1996): 37–52; and Lee Chung-Min, "China's Rise, Asia's Dilemma," *National Interest* 81 (Fall 2005): 88–94.

7. Victor D. Cha, *Alignment despite Antagonism: The United States-Korea-Japan Security Triangle* (Stanford, CA: Stanford University Press, 1999).

8. Gilbert Rozman, *Northeast Asia's Stunted Regionalism: Bilateral Distrust in the Shadow of Globalization* (Cambridge, UK: Cambridge University Press, 2004).

9. Duncan Snidal, "The Limits of Hegemonic Stability Theory," *International Organization* 39, no. 4 (Autumn 1985): 579–614.

10. Mary McEvoy Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly* 54, no. 2 (June 2010): 381–401.

11. Cameron Ortis and Paul Evans, "The Internet and Asia-Pacific security: old conflicts and new behaviour," *Pacific Review* 16, no. 4 (2003): 549–72.

12. Bruce Schneier, remarks, First Worldwide Cybersecurity Summit, Dallas, TX, 4 May 2010.

13. Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2008).

14. Kristi Govella, "Cyber Security: A New Frontier for the U.S.–Japan Alliance," Berkeley APEC Study Center, 12 May 2010, http://bascresearch.blogspot.com/2010/05/cyber-security-new-frontier-for-us.html.

15. Ronald Diebert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," International Political Sociology 4, no. 1 (March 2010): 15–32.

16. Iver Neumann and Erik Overland, "International Relations and Policy Planning: The Method of Perspectivist Scenario Building," *International Studies Perspectives* 5 (2004).

17. W. Alexander Vacca, "Cultural Constraints on Cyber Warfare: The Ongoing United States Air Force Experience," 51st Conference of the International Studies Association, New Orleans, LA, 17–20 February 2010.

18. Giulio Douhet, *Command of the Air (USAF Warrior Studies)* (Washington: Office of Air Force History, US Government Printing Office, 1983).

19. Martin Libicki, *Conquest in Cyberspace* (Cambridge: Cambridge University Press, 2007).
20. Iver B. Neumann, "Self and Other in International Relations," *European Journal of International Relations* 2, no. 2 (June 1996): 139–74.
21. W. R. Thompson, *On Global War* (Columbia: University of South Carolina Press, 1988).
22. This essay assumes that air gapping of classified and unclassified networks largely continues, but with the possibility for some bridging between them.
23. Wang Pufeng, "The Challenge of Information Warfare," *China Military Science*, Spring 1995.
24. Julian Borger, "Pentagon kept the lid on cyberwar in Kosovo," *Guardian*, 9 November 1999.
25. See Wang, "Challenge of Information Warfare."