Fall 2022

Conflict, Technology, and Integrative Thinking: The Past and Future of Geopolitical Conflict

Paul L. Johnson
Boise State University

Conflict, Technology, and Integrative Thinking: the Past and Future of Geopolitical Conflict.

Conflict, Technology, and Integrative Thinking: the Past and Future of Geopolitical Conflict.

Paul L. Johnson

College of Arts and Sciences, Boise State University

Conflict, Technology, and Integrative Thinking: the Past and Future of Geopolitical Conflict.

Abstract

Conflict is constantly evolving, and it is evolving even faster now that the world finds itself in an age where information travels at the speed of light. Scholars of military doctrine and generational warfare are currently pondering the effects of cyber warfare on the already hectic and confusing fourth generation battlespace. Invariably, generals, pundits and politicians alike in countries across the world vie to acquire these "capabilities" for their benefit and the benefit of their nation. The last time a cutting-edge advance in kinetic weaponry was made in the form of the atomic bomb, hundreds of thousands of civilian lives were taken before the international community agreed to avoid employing it even during wartime. I believe the threat posed by theorized full-spectrum cyber warfare is equally as destructive, but also insidious. In the future, military operations may rage through civilian networks. Self-driving vehicles with innocent occupants might be turned into road borne missiles for the benefit of a military commander on the other side of the globe. Strange political and social movements with no clear origin might threaten democracies around the world. Contagious messages designed to arouse the fear and hatred endemic to every human heart could envelope social media and plunge nations into war, peoples into bitter violence, and shatter ancient communities into warring factions. But I believe that unlike our progenitors -armed with Uranium warheads but with 19th century ethics- we can prevent this new evolution of warfare from causing even a paper cut. Much of the technology and concepts I will touch on also have the ability to be used to enhance our lives without being integrated into weaponry at all. I propose that the audience of this paper take it as an invitation to enhance their knowledge of the dangers posed by the defense complexes of modern nations, and to mobilize human and material resources to affect change legislatively to limit the propagation and proliferations of these new tools of destruction.

Conflict, Technology, and Integrative Thinking: the Past and Future of Geopolitical Conflict.

Keywords: Warfare, Hacking, Cybersecurity, Artificial Intelligence, Diplomacy

Conflict, Technology, and Integrative Thinking: the Past and Future of Geopolitical Conflict.

Introduction

It was around late February 2022, just about a week after my 25th birthday that the inspiration for this paper began. I was watching a news report on my phone covering the latest Russian troop movements when a clip on the television played by NBC caught my eye. Programming was supposed to be about the closing ceremonies to the Olympic games in Beijing, so I was struck to see combat footage from the 2014 Crimean conflict, a clip of Vladimir Putin speaking, and as I removed my headphones, a closeup of a lone Russian soldier holding a PKM machine gun at the ready while apparently manning a road checkpoint. I believe it was Mike Tirico who was espousing something like gratitude that the world had just gotten to watch a noble, ancient friendly competition "…as armies gather and tensons begin to flare." My usual skepticism toward mainstream reporting was not present in that moment given my own corroboration of the facts. One reliable source I followed for news about the Afghan war and another that documented world naval movements seemed to agree with NBCs assessment: the post cold war peace that the world and especially Europe had enjoyed for the last two and a half decades was coming to an end very soon.

Days later, I watched live as several dozen Russian Battalion Tactical Groups invaded nearly the entirety of Eastern Ukraine. I slept very little that night between watching updates on livemep.ua, tuning into various livestreams, and monitoring short wave radio streaming from the area to try and glean a picture of the battlespace as it unfolded real time. Such a clear window into the opening hours of a war was, I realized, unprecedented. The technology that allowed me to do this is however the same technology that is making human interaction, either peaceful or malicious, much more complex and -despite its designers' intentions- more difficult. As I watched the war in Ukraine take shape over the first few days, I also watched as the reliability of

information deteriorated. One source might say that Ukraine was days from falling, another that Russia had suffered decimating losses. Sometimes a single source even would contradict itself. I began to wonder if war had always been like this, if that was the reason for propaganda -to give anxious citizens *something* coherent to hold onto when in the fog of war, even if untrue. Has warfare now evolved to the point that confusion and chaos sewn into information and cyber systems become a weapon in its own right? Do the offensive cyber capabilities of nations and militant groups stop at military targets? If so, how? Much like ordinary citizens of western countries during the 1950s and early 1960's I find myself wondering, what is holding to world as we know it together? How does this end, and what does the future look like. I believe that these advances in warfare technology pose a great risk to our information-based civilization comparable to the threat posed by thermonuclear weapons to the world in the cold war. This is the emerging threat of fifth generation warfare. I believe that humanity can limit or even avoid this potential destruction and suffering -that we have the capacity to grow stronger than our worst impulses, and to use our creative energy for peace and discovery. But to reach this potential, I think it is important to understand how conflict has evolved throughout many generations.

William S. Lind is the policy analyst and historian from Princeton University who originated the concept of generational warfare which I will be referring to extensively. This model of modern warfare as generations has been widely adopted by the pentagon, with some adaptations. It is mainly used to categorize past, present, and future capabilities of forces and weapons systems within the context of defense research. For the purposes of this paper, warfare generations one through four are used to differentiate prevailing tactics and strategies used in conflicts. Fifth generation warfare will have its own section since it is quite nebulous and

remains elusive to define -even in academic circles. Additionally, fourth generation warfare is still unfolding, and may grow to incorporate what is now thought of as fifth generation warfare. It is helpful to think of these warfare generations in terms of the character of the conflict being studied, and not so much as an era within which the conflict occurred. For example, belligerents in contemporary conflicts may limit themselves to first of second-generation tactics depending on logistical and technological constraints present to their war effort.

First generation warfare is characterized the massing of combatant numbers ("manpower") and firepower. Most pre-industrial wars are first generational given their limited use of technology, limited use of ballistic weaponry and emphasis on strategies of attrition. The battel of Thermopylae is a great example. Second generation warfare occurs when force multipliers, be they guns, siege weapons, artillery et cetera are used to enable smaller units to inflict attrition on a much larger scale -even to numerically superior forces. The Spanish-American war and American Civil war being valid examples of 2nd Generation warfare. Third generation warfare, also called "maneuver warfare" is where we begin to see a departure from kinetic action and an emerging emphasis on utilizing high mobility to bypass defenses and strike targets beyond traditional combat lines. The German blitzkrieg and the 2003 US invasion of Iraq are strong examples of third generation warfare.

Next where things begin to get hazy since we find ourselves in the midst of a transition, either between forth to fifth generations of warfare, or far along in the fourth. Fourth generation warfare begins to encompass a great deal of kinetic conflict both organized and asymmetric instigated by nation states, terror groups, insurgent movements, and militias. Real examples of fourth generational warfare are hard to define since the nature of conflicts that are characterized by these tactics and strategies cannot confidently be called war in most circumstances due to the

low intensity and lack of major strategic goals. The Troubles in Ireland and the US occupation of Afghanistan are often referenced. The prevailing hypothesis among scholars such as Lind is that the threat of large scale nuclear warfare between superpowers made the consequences of third generation warfare unacceptable, so naturally, war became the politically nebulous venture that it has been since the end of the second world war. Finally, fifth generation warfare is theorized to be clandestine conflict enabled by cyber systems. It is either an extension directly from 3rd generation warfare tactics of threat avoidance, or a development from 4th generation tactics of low intensity and limited engagement. Little is published on doctrinal thinking that would allow much distinction between the last three generations of warfare since the 4th generation was only theorized as recently as 1989.

In these cases covering just a few hundred years, we can see the progression of warfare from essentially little more than territorial and cultural disputes, to national mobilization of entire populations and economies, to a force of destruction that has the potential to reshape the world. That potential began with atomic weaponry, and despite the falling of the iron curtain and the peaceful resolution of the cold war, this threat has not disappeared. If anything, the "attack surface" has been greatly expanded to include all manner of civil infrastructure thanks to the information age. Attack surface is a cybersecurity term used to describe the virtual size of a network's vulnerability area. An entire nation's internet can have an attack surface. In a similar way to generations of warfare, cyber threat actors' methods and motives have evolved considerably throughout the existence of the internet. Traditionally, threat actors have targeted both enterprises and individuals on a rather limited scale to extort money, gain access to privileged information, exert control over systems and data, or disrupt the function of a cyber system. This activity was given the name "hacking" back in the late 1980s. As the name implies,

early hacking techniques were anything but elegant, and they were rarely subtle if they happened to be observed in use by authorized users of a system being hacked. What began as something of a fun, prank-like activity for eccentric tech savvy young people, however, steadily morphed into a potent tool of exploitation by actors ranging in motive from mischievous to nefarious. To be clear, most hacking that occurs is rather innocuous, though often unethical, ranging from cheating in videogames to bypassing paywalls on entertainment sites. Increasingly however, shadowy groups claim responsibility for massive data breaches, identity theft, blackmail, and disruption of infrastructure. For one example, in 2020 the hacking group "Anonymous" claimed responsibility for jamming the Chicago Police Department's citywide radio network by playing several anti-police songs on repeat for around 3 hours. This jamming of communications occurred during an unlawful assembly that led to a destructive demonstration, possibly exacerbated by Anonymous' involvement. Interestingly, this event mirrors military tactics of playing adversarial messages through music or voice, such as those exercised by US Army and Air Force electronic warfare (EW) units during war games. This incident, along with the Colonial Pipeline shutdown and the leaked NSA virus that become known as "WannaCry" are good examples of mid-level, high visibility threats that impose disruptive consequences on private and public target organizations. Unfortunately, the threat doesn't stop there, since military and civil think tanks are hard at work developing methods to deliver information and psychological payloads to targets, as well as stealthy viruses to hobble and even destroy industrial infrastructure.

Recall that in fifth generation warfare, there are no front lines. Conflict has steadily evolved away from afflicting devastating attraction, to outmaneuvering opponents, to -it appears- exploiting opponents and nullifying their defenses before they even know there is a war on.

Conflict, Technology, and Integrative Thinking: the Past and Future of Geopolitical Conflict.

Again, whether this is an extension of 4th generation warfare, or the corner being turned to 5th generation warfare is a matter of ongoing debate, but it is certain that this method of warfare is as revolutionary as the blitzkrieg strategy. The 2011 Stuxnet attacks are a rare glimpse of the capabilities being developed by nations to impact their enemies. The Stuxnet worm is believed to have been developed jointly by the United States and Israel since it was discovered to have infected Iran's nuclear enrichment centrifuges. Specifically, the worm is designed to exploit a vulnerability in a Windows supervisory control (SCADA) program that allows the malicious code to be passed to Siemens' software used by an electromechanical device known as Programmable Logic Controller (PLC). PLCs built by Allen-Bradley and Siemens are ubiquitous in nearly any industry that requires automation of processes, from wastewater treatment to electrical power distribution. These are known in cybersecurity as industrial control systems, or ICS. After moving from Window's to the "Step7" software in the PLC device, the virus can collect information about traffic on the ICS network, as well as modify parameters within the PLCs programming. In the case of Iran's nuclear centrifuges, the PLCs controlling the drums were set to a speed just above the maximum limit for the centrifuge so that they slowly destroyed the expensive, purpose-built machines. All the while, the system appeared to technicians as though nothing was out of the ordinary at all. Looking at Stuxnet, it isn't hard to imagine how this tactic may have been improved over the last 12 years. Plenty of industrial infrastructure can be hijacked in a similar manner to have devastating consequences in terms of casualties, causing damage to an enterprise's reputation, or even interruption of an entire nation's power grid. Cyber warfare alone is damaging enough, but when combined with traditional tactics of warfare and geopolitical maneuvering (as the term "full spectrum" is meant to denote), it has the potential to multiply the destructive force of human conflict in irrevocable ways.

Conflict, Technology, and Integrative Thinking: the Past and Future of Geopolitical Conflict.

Conclusion

So, what is my purpose behind this? Simply, to inspire action. We now live in an age where personal communication enabled by internet connectivity can travel as fast or faster than the classic narratives projected by nations and politicians. One major thing that has changed in the last few centuries of human conflict is that now people rarely go to war with each other, but instead it is governments and rulers that compel their citizens to take up arms against neighbors. Another benefit of our lightspeed communication is that the international community is globalizing at a steady pace, bridging historical social and geographical boundaries between people. While many people still prefer to keep to their traditions and customs, people of the world are slowly but surely finding that we have more in common with each other than not and interacting with others accordingly. The liberalization of the world has the potential to be one of the great miracles of human history and barring the fading desires of a shrinking elite to forcibly bring the world under a single techno-capitalist rule, we are much more likely to enter a collaborative, pluralist future where conflict and organized violence are viewed as the costly, wasteful and fruitless endeavors they are. But that only happens when those of us with the power to change the world act with the best intent, not only for ourselves, but for others vastly distant and different from us around the world, and those to come. Cyber technology is like any advancement in human technology since the discovery of fire. The AIs that I mentioned *could* be used to plan and wage unlimited, low intensity warfare on a global scale, but they might also identify patterns of innocuous behavior that when distilled and viewed on a correlative framework, could be a recognizable pattern leading to deadly accidents and thus help us take action to prevent disasters. The intelligence gathering tools used by hackers could help first

responders to track down malevolent actors, or help journalists expose unethical practices in business or government. The key is that we, who vote and engage in advocacy in our democratic nations remain aware of the potential of emerging technologies and attempt to restrain those who would do harm with them while encouraging the efforts of those who would do good. History shows us that the best ideas usually win, and I believe that will hold true still. Specifically, for me, this research has helped me to articulate my resolve to never use my skills to create machines for the purpose of hurting people, deceiving them or manipulating them. I believe that I will be successful in promoting this sentiment to other automation and security professionals. Much as healthcare workers take the oath of Hippocrates to “do no harm”, I believe people like me should do the same, and encourage others to follow. The world would never fully recover from the consequences of cyber technology being unleashed for the purposes of destruction.

Conflict, Technology, and Integrative Thinking: the Past and Future of Geopolitical Conflict.

References

1. Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports, 5*, 100167. doi:10.1016/j.chbr.2022.100167
2. De Santo, D., Malavenda, C., Romano, S., & Vecchio, C. (2021). Exploiting the MIL-STD-1553 avionic data bus with an active cyber device. *Computers & Security, 100*, 102097. doi:10.1016/j.cose.2020.102097
3. Desouza, K. C., Ahmad, A., Naseer, H., & Sharma, M. (2020). Weaponizing information systems for political disruption: The actor, Lever, effects, and response taxonomy (alert). *Computers & Security, 88*, 101606. doi:10.1016/j.cose.2019.101606
4. Lind, W. S. (2012). Unfriendly Fire. American Conservative, 11(7), 7–9.
5. Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers & Security, 31*(4), 418-436. doi:10.1016/j.cose.2012.02.009
6. Sotelo Monge, M. A., & Maestre Vidal, J. (2021). Conceptualization and cases of study on cyber operations against the sustainability of the Tactical Edge. *Future Generation Computer Systems, 125*, 869-890. doi:10.1016/j.future.2021.07.016

7. WANG Guang-wei, PAN Hong, & FAN Ming-yu. (2014). Dynamic Analysis of a Suspected Stuxnet Malicious Code. Research & Exploration in Laboratory, 33(8), 119–122.