Space and Defense

Volume 12
Number 1 *Winter 2021*

Article 1

March 2020

Space and Defense – Volume Twelve – Number One – Winter 2021

Space and Defense Journal

Recommended Citation

Space and Defense Journal (2020) "Space and Defense – Volume Twelve – Number One – Winter 2021," *Space and Defense*: Vol. 12 : No. 1 , Article 1.
Available at: https://digitalcommons.unomaha.edu/spaceanddefense/vol12/iss1/1

SPACE & DEFENSE

Volume Twelve Number One Winter 2021

EISENHOWER CENTER
FOR SPACE AND DEFENSE STUDIES

Space & Defense

Journal of the United States Air Force Academy
Eisenhower Center for Space and Defense Studies

Publisher

Col. Kris Bauman, Kris.Bauman@usafa.edu
Director, Eisenhower Center for Space and Defense Studies

Thank You to Our Reviewers

Andrew Aldrin
United Launch Alliance

James Armor
ATK

Steven Beard
Univ. of California San Diego

William Barry
NASA

Daniel Blinder
UNSAM-CONICET, Argentina

Robert Callahan
NORAD-NORTHCOM

James Cameron
Fundação Getúlio Vargas, Brazil

Robert Carriedo
U.S. Air Force Academy

Dean Cheng
Heritage Foundation

Christopher Culver
U.S Air Force Academy

Frans von der Dunk
University of Nebraska

Christopher Dunlap
Naval Postgraduate School

Paul Eckart
Boeing

Andrew Erickson
Naval War College

James Fielder
Colorado State University

Joanne Gabrynowicz
University of Mississippi

Jason Healey
Atlantic Council

Stephen Herzog
Yale University

Theresa Hitchens
United Nations, Switzerland

Wade Huntley
Independent Researcher, USA

Lauren Ice
Johns Hopkins Applied Physics Lab

Ram Jakhu
McGill University, Canada

Dana Johnson
Department of State, USA

Jaclyn Kerr
Lawrence Livermore, CGSR

Roger Launius
National Air and Space Museum

Charlotte Lee
Berkeley City College

John Logsdon
George Washington University

Laura Delgado Lopez
Secure World Foundation

Adam Lowther
SANDS, Kirtland AFB

Agnieszka Lukaszczyk
Secure World Foundation, Belgium

Molly Macauley
Resources for the Future

Torey McMurdo
Yale U. / U.S. Naval War College

Clay Moltz
Naval Postgraduate School

Scott Pace
George Washington University

Xavier Pasco
Foundation for Strategic Research, France

Elliot Pulham
Space Foundation

Wolfgang Rathbeger
European Space Policy Institute, Austria

Andrew Reddie
University of California, Berkeley

John Riley
U.S. Air Force Academy

Chiara Ruffa
Swedish Defence University, Sweden

Victoria Samson
Secure World Foundation

Jaganath Sankaran
Los Alamos National Laboratory

Matthew Schaefer
University of Nebraska

Benjamin Shearn
George Mason University

Rouven Steeves
U.S. Air Force Academy

Dimitrios Stroikos
London School of Economics, United Kingdom

Brent Talbot
U.S. Air Force Academy

Susan Trepczynski
United States Air Force

Scott Trimboli
University of Colorado, Colorado Springs

James Vedda
Aerospace Corporation

Rick Walker
Digital Consulting Services

Annalisa Weigel
Massachusetts Institute of Technology

David Whalen
University of North Dakota

George Whitesides
NASA Headquarters

Ray Williamson
Secure Word Foundation

*This is the authoritative Eisenhower Center for Space and Defense Studies/U.S. Air Force Academy edition of *Space & Defense*. *Space & Defense* should be acknowledged whenever material is quoted from or based on its content. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and, unless otherwise specified, do not reflect official views of the U.S. Government or the U.S. Air Force Academy.
Space & Defense is available at https://www.usafa.edu/research/research-centers/eisenhower-center-space-defense-studies/ and indexed by ©EBSCO*host* and the University of Nebraska Omaha *Digital Commons*.
United States Library of Congress, ISSN 2380-131X.

Editor, *Space & Defense*
Dept. of Political Science
2354 Fairchild Dr., Suite 6L-116
USAF Academy, CO 80840

Space & Defense

Journal of the United States Air Force Academy

Eisenhower Center for Space and Defense Studies

Volume Twelve ▪ Number One ▪ Winter 2021

Senior Leader Voice

Articles

Essays

Editor's Note

In this issue, we extend our approach to *Space & Defense* as a challenge within the broad field of inquiry known as political economy. By this we mean that national defense of "spaces" or multiple domains for national security involves more than allocating resources and executing programs for increasing military capability. It also entails thinking through strategic problem sets that include elements of cooperation—international alliances and domestic negotiations—as well as competition among military organizations.

Consistent with our aim to open the journal's editorial scope and address all relevant frontiers of defense policy, this issue welcomes contributions on space, cyber security, artificial intelligence and nuclear deterrence. General John E. Hyten, then-commander of U.S. Strategic Command, addressed cadets at the U.S. Air Force Academy (USAFA) for the 2019 Eaker Lecture on preparing to meet the 21st century deterrence mission. He has graciously allowed *Space & Defense* to publish a lightly edited transcript of his remarks to future Air and Space Force officers.

In our first feature article, Roger Wortman of the U.S. Space Force reflects on the mission of defending vulnerable satellites on orbit. He draws inspiration from a popular fictional tale, *Defence of Duffer's Drift*, to explain how military science may be supplemented by game play that entertains a type of dream world based on reality but flexible with respect to counterfactuals for adversary plans of attack. Implications for developing USSF strategy, operational art, doctrine, and adaptability in crises ought to hold, regardless of whether or when international powers choose to weaponize space.

Abderrahmane Sokri extends the theme of imperfect defense to the cyber domain. He uses a clever application of the business-based leader-follower equilibrium from economic theory to explore the possibility of a Goldilocks solution for cyber defense. As in the classic Stackelberg competition, first mover's optimal strategy is not to invest everything he has, for there will be diminishing rate of return on how much he deters his adversary. With relatively few, plausible assumptions on how investment improves resilience of cyber networks for defender, and limits benefits for attacker, Sokri conjures a game-theoretic world that offers insights as to how defender can calibrate just-right spending on cyber defense and (unlike cyber offense) advertise his effort with intent to lock an adversary into predictable equilibrium play.

In this issue, we present two remarkable cadet papers nurtured by USAFA's Nuclear Weapons and Strategy minor and recognized by external experts on deterrence. Second Lieutenant Marshall Foster (USAFA '20) reviews the burgeoning literature on how artificial intelligence will affect strategic stability and supplies his own account based on the interaction of strategic cultures. Second Lieutenant Liam Connolly (USAFA '19) surveys recent pressure on Baltic states within NATO and raises the importance of national resilience—a rather complex correlate of defense spending—for the success of U.S. extended deterrence in Europe.

Finally, as contributing editor, I review *The Death of Expertise* (Oxford, 2017) by Naval War College professor Tom Nichols. Nichols in the book is mainly concerned about how status decline of experts in American society imperils modern democracy, which depends on elected representatives as generalists, weighing competing advice from professionals or accepting political risk in order to follow the truth presented by expert consensus. Many of Nichols' examples land in the policy areas of health, education, and economy, but as an international security scholar, he is aware of additional implications from the death of expertise for foreign policy and U.S. strategic competence. Nichols' challenges, I argue, are important for civilian analysts and military officers, the relevant experts, to keep at the forefront as they prepare the new Space Force, against rapidly evolving threats, under democratic civilian control and subordinate to the authority of elected politicians.

In my case, as is true for all our authors, *contributions herein are academic and do not represent official policy or opinion of the U.S. Air Force or the U.S. Space Force.*

Damon Coletta
USAFA
January 2021

As Delivered Remarks

Gen John E. Hyten

On 23 April 2019, Gen Hyten, commander of USSTRATCOM, visited the Air Force Academy to give the annual Ira C. Eaker lecture on National Defense Policy. Before soon to be graduates and officers, Gen Hyten discussed how several Air Force career fields, particularly those involving missiles and space, contribute to successful deterrence in the 21st century. -Editor

Location: U.S. Air Force Academy, Colorado Springs, Colorado
Event: Eaker Lecture on National Defense Policy (Edited Transcript for Clarity)

…I always thought, many times as I look back, if life would have been different if I'd gone to the Air Force Academy because one of the big advantages you guys are about to experience as you go into the world, into the United States Air Force, is that you will have a support structure built in from the day you come into the service. You will have this group of people that you had a common experience with for your four years. As you go through that structure you will have that common bond that will pull you together. It's an amazing thing. I didn't have that.

I was the first class back into Harvard after the Vietnam riots. We had nine students that were in ROTC [Reserve Officers' Training Corps] that cross-enrolled in MIT [Massachusetts Institute of Technology] when I first started. A month into the program there were only five because we got kicked, cursed, spat at, assaulted, all on the streets of Cambridge, Massachusetts, just because we were wearing the uniform of our nation's country. Four of my classmates decided they'd figure out some other way to pay, but I couldn't afford Harvard unless the Air Force paid for it. So we stayed, the five of us stayed. Now, the other four are gone as well, and none served 20 years. So, I don't have any classmates still serving. You guys will have classmates all the way through that you get to deal with.

…And it's a special place that you're about to join. Whether you're '22, '21, 2019, wherever you are, you're about to join the United States Air Force and I hope you enjoyed some of the pictures that were in that video you just looked through. Pictures of the most powerful combatant command in the world, my command, U.S. Strategic Command. It is simply the most powerful command that's ever been created. Some of my friends don't like it when I say that, but it's simply the fact. It's true. That's who we are.

But, I want you to think back just a short period of time in our history when just over a decade ago that command with all the capability you just saw was dying on a vine. It had huge problems. It had morale problems across the entire force. It got to be so bad, we loaded a nuclear weapon on a B-52 and flew it from North Dakota to Louisiana, and until it got to Louisiana nobody even knew we did it. We sent missile parts from Hill Air Force Base in Utah to Taiwan, and didn't even know we did it – nuclear missile parts. We had huge cheating scandals in the nuclear force on the Navy side as well as the Air Force side.

How could that happen? How could the most powerful command in the United States end up with those kinds of problems? It did because we took our eye off of what the most important thing in our country is, and the most important thing in our country is our nation’s security. Our nation’s security is guaranteed by the capabilities of U.S. Strategic Command.

We had senior leadership at a northern-tier missile base who stood up in front of a bunch of ICBM [intercontinental ballistic missile] operators, a bunch of missileers, a bunch of the finest people that the nation’s ever produced, and said you guys need to get out of the missile business and get into the space business because the missile business is dying and the space business is where it’s going to be happening. That’s not a great way to deal with the most important mission in the United States Air Force, to tell the people that actually do it that they’re a dying mission.

It’s not a dying mission. It’s the most important mission that we have. Nuclear deterrence is what this nation’s defense is based on. From beginning to end, that’s where it starts. And if you don’t understand that, you don’t understand the concept of military power; you don’t understand the concept of deterrence. Nuclear capabilities are essential to our nation’s security. And a lot of people still question that. But you’re about to enter an Air Force where that nuclear business is critical to everything that we do, and you need to understand what that is.

One of the questions that I get more often than any other question is can you, me, imagine a world without nuclear weapons? And the answer is yes. I can imagine a world without nuclear weapons and everybody in this room can imagine a world without nuclear weapons as well. Because you know what that world looks like? The world before August of 1945. Somewhere in high school history or here at the academy you’ve studied a little bit about World War II. So let’s just think about the numbers of World War II for a second.

Between the years 1939 and 1945 the world killed somewhere between 60 and 80 million people in World War II. Think about those numbers. Sixty to 80 million people killed in a war.

If you do the math, that’s about 33,000 people a day being killed in World War II. If you think about this nation’s horrible experience in Vietnam, and all the heroes that we sent, our nation’s greatest treasure, our sons and daughters into Vietnam to fight for our freedoms, in that horrible experience we lost 58,000 Americans – 58,000 of our sons and daughters. That’s two days of violence in World War II. Two days. Imagine every day that goes by and it’s the entire destruction of the Vietnam War. Ever since nuclear weapons were invented that level of destruction went away. It went away because the nations that had those nuclear capabilities always had to be worried about whether they were going to cross the line that would cause their adversary to want to use nuclear weapons back against them. That’s the basis of deterrence.

The basis of deterrence is having a capability that is so fearful that the adversary won’t cross that line and won’t ever walk down that path. That’s what we want to have happen. But in order for deterrence to work, we have to be ready to fight that nuclear war each and every day and that’s the pictures you saw on the screen. The Soldiers, Sailors, Airmen, Marines of U.S. Strategic Command practicing that mission every day so that our adversaries see it and they know it and they won’t walk down that line. That’s what nuclear weapons mean in the world of the 21st century.

But we took our eye off it because 9/11 happened. And most of the people in this room have no memories of the world before 9/11/2001 because you are not old enough. And because you don't have those memories your entire experience has been focused on the Global War on Terror. And as we walk into the future, that global war on terror is not going to go away. We've had great success on the battlefield in Syria. Great success on the battlefields of Iraq. Afghanistan is reaching a place where we're talking peace with the Taliban. All those things are looking good, but I tell you what, terrorism is not going away. Terrorism is at least a generational thing. Terrorism is something that you're going to have to deal with your entire time in the military whether it's a four-year plan like I had or a 42-year plan like I ended up. Whatever that plan is, you're going to be dealing with terrorism that entire time.

But here's an interesting thing about the terrorists that want to attack the United States. They will never be able to defeat the United States of America. Ever. We have to protect our citizens, we have to protect our capabilities, and they want to terrorize us, they want to damage us. They're going to do those things and we're going to fight and defeat them wherever they happen to be. But they are not an existential threat to this country.

There's only two nations on the planet right now that bring that existential threat who have a stated purpose of defeating the United States. The stated purpose to change the world, to change the entire world order, put their model on the world order, and not the United States model, not the Western model, not our ally model, not the NATO [North Atlantic Treaty Organization] model, and that's Russia and China. Russia and China are once again recognized as potential adversaries of the United States.

Russia all of a sudden became that adversary again in 2014 when they invaded Crimea. In 2014 they invaded Crimea. They were our adversaries then. Somehow that was news. If you actually read what the President of Russia has said multiple times, as early as 2000. … Vladimir Putin was elected President of Russia in March of 2000. In April of 2000 he gave a speech. In that speech he said they'd been watching the United States. They'd been watching NATO.

They've been watching what we've been doing in the first Gulf War, in Allied Force. Now, this was before 9/11. They hadn't yet seen how we fought in Iraq and Afghanistan. But they understood that we had built this unbelievably powerful conventional force. And because of that powerful conventional force they were going to have to change their doctrine and focus on their nuclear and strategic capabilities. They were going to modernize their nuclear capabilities, and build a large number of low-yield nuclear weapons as well. They would also reserve the right to deploy those low-yield nuclear weapons on a battlefield in Europe should Russia be challenged. That doctrine began in April of 2000.

In 2006, Putin announced the full modernization of the nuclear force, saying the modernization would be done by 2020. I won't tell you the classified numbers, but they're going to be pretty close to being done by 2020. They've made multiple speeches over the time – Putin and the other leadership of Russia –that this would be their strategy. But somehow they were our friend. They were our friend all the way up to 2014 when suddenly they became a potential adversary again when they invaded Crimea. That was just the same part of the strategy they've announced for the 14 years prior to that ever since Putin was elected.

This is an adversary we're going to have to deal with, and this is an adversary you're going to have to deal with. And you better study your adversary. You better understand the way they think, why they think that way, what they're doing. Look at them as an adversary.

Look at China. China's suddenly an adversary of the United States again as well. Somehow that's news as well. The first time I wrote about China was 1998, and I'll give you warning, if you ever write when you're going to graduate school, you go on to a fellowship, or you write a thesis, you better be aware that somebody's actually going to read that someday and hold you accountable for what you write down.

But, I wrote down in a paper in 1998 what I thought China was going to be doing in space and what China was going to be doing as far as their overall strategy. And you know where I got that? I got that from the Chinese publications that had been already written. I got that from the Chinese students at the University of Illinois I was going to school with. They stated exactly what they were going to do and they've been doing it for the last 20-plus years without fail on that same strategy. You can find everything that they're doing right now in the strategy that was written in the 1990s, and we just ignored it as a nation. And we helped China build their power. Now, China wants to become the regional power in the Pacific, and now they've started to write about being the global power by the end of the century.

That's the world that we live in. Why are they building islands in the South China Sea? It's part of that same strategy. Why are they building space weapons? It's part of the same strategy. Why are they building aggressive cyber capabilities? It's part of the same strategy. And they wrote it down over 20 years ago. But nobody read it.

So, you better study your adversaries and understand the way they think, the way they are organized, the way they are trained, and the way they're equipped, because someday we may have to deal with them.

The other piece of the puzzle is to somehow make sure we never have to deal with them, which brings us back to deterrence. The last thing we want to do in this world is go to war with Russia and China. That's the last thing we want to see happen. If anybody thinks that that's a good thing for the world you don't live in the same world I do. We have to make sure that never happens, and you do that with deterrence.

So, deterrence in the 21st century has been a fascinating discussion. A fascinating discussion because of the lack of discussion. So, somehow deterrence in the 21st century is looked at as STRATCOM's job. General Hyten, you're the STRATCOM commander, deterrence is your job. And if you read the Unified Command Plan you'll find that. That's my number one job, strategic deterrence.

Somehow people think that just because we have 1,550 deployed nuclear weapons and comply with the New START [Strategic Arms Reduction] Treaty we deter all our adversaries, and all you have to do is pick up a newspaper and read just the beginnings of that to understand that's not true. We don't deter all behavior because of the existence of nuclear weapons.

So, what is strategic deterrence in the 21st century? When I came into command in 2016 we started asking that question. We built an academic alliance with 35 colleges and universities to start looking at what is deterrence in the 21st century. And we intentionally didn’t give anybody any answers when I started just asking the question. What is deterrence in the 21st century? Just to try to create a debate. And I would go to places that fundamentally disagree with the way I think about nuclear weapons. I would go to Stanford and Yale and Harvard, and I would debate the facts with them. I would debate with people that have differences of opinion to me about what deterrence is in the 21st century to try to gather that broader discussion of what goes on.

If you want to know where the strategic deterrent theory began, it began in colleges and universities and the think tanks in this country like RAND, in the early 1960s with Herman Kahn and Thomas Schelling, Bernard Brodie, many of the folks that you’ve read in your classes here in this institution came from that. And when you start thinking about deterrence, you go back and read them, because there hasn’t really been anybody in the 21st century that is of their element. But we are starting to see that change. We’re starting to see the beginnings of a new debate at Georgetown and Stanford and elsewhere, about different perspectives of what deterrence is in the 21st century.

And here are the elements. Deterrence now is a multi-polar problem. Because, you just can’t focus on Russia and say New START is a global arms reduction treaty. It’s not. It’s just two nations. But everything we do with Russia impacts China. Everything we do with North Korea impacts Russia. Everything we do with Russia impacts China. It just goes all the way around. So we have to think about everything that we do in this multi-polar world.

The second piece, it is multi-domain. It is all domains. All the domains have to come into fruition. And you’ve heard the Air Force concept of Multi-Domain Command and Control. The Army has a concept called Multi-Domain Operations. The Navy is working fleet command and control issues. All trying to get at the same issue.

But here’s where the challenge really is as we go forward. The challenge is how do we integrate global capabilities? How do we integrate what the Chairman calls global fires? Because if we ever get into a conflict with an adversary, there’s going to be non-kinetic and kinetic shooting happening in space, cyber, air, land and sea all at the same time, and we have to figure out how with multiple commanders involved we integrate all those capabilities together.

So, you want to know what you have to do in order to become a great joint officer? Just become a great Airman. This institution is not building great joint warriors. That will happen down the road. We’re getting you ready to be Airmen.

Now, there are other services in this room that are going as exchange programs in here. When you go back to your service, whatever service you came from, become a great Soldier, a great Sailor, a great Airman, a great Marine, because what I want as a joint commander is I want to pull the best domain expertise I can from every domain that we operate in, put them all together in a room and then figure out how to fight together effectively in all those domains. But what I don’t want, is I don’t want somebody that knows a little bit about every domain. I want a room full of people that know everything about each domain and then we’ll figure out how to pull those pieces together.

So, the first thing you’ve got to do is become an expert in whatever career field you’re going into. If you’re going to be a pilot, become the best pilot in the United States Air

Force. And if you're going to be a pilot, that should be your goal. Not just be a good pilot, but be the best pilot in the United States Air Force. The best pilot in the United States military. If you're going into space, become the best space warrior there is. If you're going into cyber, become a cyber killer. If you're going into intel, become the best intel operator there is. If you're going into acquisition, if you're going into engineering, become the best. Learn that. That's what you have to do for the next 10 years. Then when the time comes we're going to take that expertise and we're going to put it to use. But you should never lose that expertise because that will define who you are. And in your soul, in your heart as you go forward into the future, you need to resonate those values. Because when I look at myself in the mirror, even though I'm a joint commander, even though I command Soldiers, Sailors, Airmen, Marines, my professional identity is an Airman, and it always will be. That's the way it's got to be.

And yes, I have a deep space background. And a couple of weeks ago, the day after I was supposed to be here the last time when I left because of the storm that came in, I was testifying with my bosses, the Secretary of Defense and the Chairman of the Joint Chiefs, the Secretary of the Air Force, in front of the Senate Armed Services Committee on the future of space, and I know that subject well. I have a vision of what that future's going to be. We're going to make space a real warfighting domain because it basically already is. The rest of the world just doesn't understand it. We're going to walk into it.

But, I was challenged about my background as an Airman, whether the Air Force was the right place for space. I said, you understand that when I bleed, I bleed blue because I am an Airman through and through. But I know we have also reached the point where space has to be treated as its own domain, just like the air was, just like the maritime domain was, because it is a place where we're going to fight and it's a place we're going to have to win, an Air Force that we're going to build around it, and I believe the fact that it's still going to be in the United States Air Force is exactly right.

We're going to get into Q&A in a minute, and that's my favorite part, so we're going to have plenty of time for Q&A. But I would ask you to identify yourself. I'm going to ask you some questions here and I don't want you to raise your hand, I don't want you to embarrass yourself, I don't want you do anything stupid. But I'm just going to ask you some basic questions that every Airman should know the answer to. This is our history. This is our history as a United States Air Force and you should know these names off the back of your hand. And if we're not teaching you these names at the Air Force Academy we're doing something wrong. But this is the basics of who we are.

I'm going to ask you the easy question first. That is, who is the father of space and missiles in the United States Air Force? That's the easy one. That's Gen. Bernard Schriever.

Gen. Bernard Schriever basically invented the ICBM. He invented the spy satellite. He invented the rocket inside the military. He's the guy that was there. One of my great experiences of my life was as a young major to be told by the Chief of Staff of the Air Force, Gen. [Merrill] Tony McPeak – I was the idiot major in that story, by the way, but I don't need to go into that. But going to Andrews get a C-21, taking off to California, pick up Gen. Schriever and take him to places X, Y, and Z and show him what we're doing in space in the United States Air Force. General Schriever was criticizing the Air

Force and General McPeak. I got to sit in the back of that C-21 and receive a lecture from Gen. Schriever that I'll never forget because he told me how we were screwing up in the Air Force, not treating space the way it should be treated. So he was the father of space and missiles.

Here's a second question. I'm going to make you raise your hand real quick. How many in here are aerospace engineers? A bunch of you. Who invented the term aerospace? <pause>

Gen. Thomas D. White, Chief of Staff of the Air Force, fourth chief of staff, 1959. A hearing in front of Congress. Eight times during the hearing he used the term 'aerospace,' as the indivisible spectrum of operations from air to space that has to happen for the United States Air Force to control the high ground of the future.

A funny story-- Gen. [Dwight] Beach, an Army general testifying a short time later. They asked General Beach, General White keeps using this term aerospace. What do you think about that term? And seriously, you can look it up in the Congressional Record, General Beach goes, "I always heard of armospace."

Armospace didn't stick. Aerospace stuck. Because air and space are the areas we have to control.

Who is the general most responsible for creating Air Force Space Command? The command I commanded until 2016. Gen. [Jerome] Jerry O'Malley, commander of Tactical Air Command. The fighter pilot's fighter pilot. When he was a wing commander at Beale, he flew the SR-71, the U-2, he got read into these classified space programs, and he looked at it and said there's all this space stuff going on but none of it gets to the warfighter. So, when he became the XO [director for operations] of the Air Force, now the A3 of the Air Force, he started working with the chiefs of staff, one of them being [Gen.] Lew Allen, and said we need to create a command that is focused on the operational application of space to the battlefield. That would be Air Force Space Command.

Here's the thing about those three people – General Schriever, General White, General O'Malley – they were all fighter pilots. They were all pilots. And somehow the popular culture has reached the point where somehow the world doesn't think that pilots care about space and that's so untrue. Not only do they care about space, our chief of staff cares about space as much as anybody I know; the general officers I work with care about space as much as anybody I know. But it was actually invented by pilots because that was the future of the United States Air Force. That's where we're going to go. And everyone in this room should be able to tell that story.

And what is it all about? It's all about our nation's most important mission. It's all about strategic deterrence in the 21st century, because strategic deterrence is going to come from being able to control the air, control space, control cyberspace, having a nuclear deterrent that is ready and able to respond to any threat. That is the structure that we're going to have. That's where it all comes together. And that's what you need to know when you go into the Air Force and you become second lieutenants. And you're not going to think about it for a while. You're just going to think about flying planes, and operating satellites and operating in cyberspace, and providing intel and building stuff. That's what you're going to think about for the next decade and that's great.

But if you remember nothing else from today, remember that we have adversaries in this world that we don’t want to go to war with. The only way to avoid that war is be ready to go to war and to defeat them in a war on any day that the nation requires us to. That’s what we’re supposed to do in the United States Air Force. That’s what we’re supposed to do at STRATCOM. That’s what we’re supposed to do in the United States military, and we need to be ready to do that.

I will stop there and just say thanks for the decision that you’ve made to come to this institution. Thanks for what you’re about to do as you go forward into whatever service, whatever nation, whatever structure you’re going into. But if you’re going into the Air Force, understand that we just want you to be great Airmen, because great Airmen and great Soldiers, great Sailors, great Marines are what makes a great joint force – not great joint warriors.

Duffer's Drift and Space Operations

Roger Wortman

Defence of Duffer's Drift*, a popular Boer War tale among British infantry officers, teaches lessons for the future of space operations.*

Published in the early 20th Century, *The Defence of Duffer's Drift* is a work of fiction written as an educational tool for small unit leaders.[1] The novella outlines the experiences of a young lieutenant and his tumultuous path to success when charged with defending key terrain. Told through a series of dreams, *Duffer's Drift* provides multiple tactical lessons through an iterative process, each building on the previous sequence. The officer fails multiple times while learning from various mistakes while incrementally moving toward success.[2] Although the work focuses on ground combat and maneuver warfare, the principles addressed can be applied to a variety of fields. As such, *Duffer's Drift* is often suggested as professional development reading for many service members regardless of career field.[3]

The author, British Army Captain Ernest Dunlop Swinton, based the story on his own experiences during the Boer War of 1899-1902. Although *Duffer's Drift* draws from Swinton's days as a small unit leader, lessons within the tale move beyond tactical considerations and reinforce a wide array of combined arms principles. This enriches the story while also foretelling Swinton's eventual career progression as a professor, historian, war correspondent, and a forefather of armored warfare. Eventually attaining the rank of Major General, Swinton retired in 1919 and is considered one of Britain's leading military thinkers. [4]

The structure and flow of *Duffer's Drift* is reminiscent of a short autobiography vice an instructional pamphlet. Its first person narrative invites the reader to trust the author's authenticity while remaining open to the ideas and education provided through each dream sequence. Its time loop plot device is instantly recognizable by modern readers, although Swinton's pacing and adjustments through each dream enable the story to unfold naturally while avoiding needless repetition. At thirty-two pages, *Duffer's Drift* uses this simple and effective storytelling technique to educate the reader on the complexities of ground warfare. Additionally, this literary approach provides easy to absorb lessons and professional education for all ranks and career fields.

LESSONS OF DUFFER'S DRIFT

The story's protagonist, Lieutenant Backsight Forethought, leads a light infantry unit deployed to southern Africa in service of the British Empire. Although the backdrop for *Duffer's Drift* is the Boer War circa early 1900s, the tale avoids commentary on geopolitical issues or reasoning for the

[1] Roger Wortman is a civilian analyst with the U.S. Space Force. This article was written and submitted prior to him joining the service.

[2] Swinton, Ernest, "The Defence of Duffer's Drift," Department of Defense FMFRP 12-33, 1989. First published 1904.

[3] Baker, Deane-Peter, "'Dreams of Battle': A Small Window into the Evolution of Us Army Tactical Ethics, 1921-2009," *Journal of Military Ethics* 13, no. 4 (2014): 302.

[4] Tucker, S., 500 Great Military Leaders, ABC-CLIO, LLC, 2014.

conflict.[5] Instead, the focal point of the story is how the officer navigates the complexities of warfare. The story itself begins with the lieutenant falling asleep after arriving at a river fording site he and his fifty men are charged with defending. Each vivid dream sequence pertains to the defense of the drift; and each sequence results in disaster for the lieutenant's men and mission. Yet, as the dreams progress, the lieutenant applies lessons learned to the subsequent scenario. A clear example is seen in the first dream sequence and its influence in decisions made in the second iteration.

In the first dream the lieutenant waits until the next day to begin defensive preparations. Sentries are placed around his forces to provide security; though little thought is employed to their positions. He allows local salesmen into the encampment to barter with his men. Tents are erected in plain view and consolidated. The enemy soon arrives; the battle is quick and destructive. The British element sustains multiple casualties and those who survive become prisoners. Reviewing his actions during defensive preparations, the lieutenant identifies four lessons learned:[6]

- Do not delay in preparing defenses.

- Placement and concealment of sentries is critical.

- Do not allow anyone other than your own forces into the perimeter.

- Concealment in tents does not provide cover.

The second dream serves as a reset of the battlefield. With a fresh complement of forces at his disposal, the lieutenant incorporates previous lessons. He begins defensive preparations immediately, keeps locals out, properly prepares sentries, and ensures his men can fit into the entrenchments to defend against enemy fires. The enemy eventually attacks, and Lieutenant BF's unit is again overrun. However, the lieutenant reviews what happened and identifies lessons learned to be applied at the third iteration.

The series of dreams ends after six cycles, each building on previous events. Throughout the novella concepts such as defense against heavy weaponry, operational security, management of the local population, seizing the initiative, and many others are identified by the lieutenant. Every learning point is incorporated in the following defensive plan, and on the sixth dream the British defense succeeds. Despite this story being over one hundred years old, *The Defence of Duffer's Drift* remains relevant to modern battlefields.[7] The iterative nature of the narrative structure combined with an almost scientific approach to testing and validation proves its value as an educational tool and timeless classic for any maneuver warfare officer. Moreover, the lessons included in *Duffer's Drift* are not limited to educating infantry professionals. Concepts such as placement of forces, operational security, involvement of local populations and more are facets of warfare that apply to every career field, even space professionals.

VALIDITY IN THE SPACE DOMAIN

The U.S. Department of Defense (DoD) conceptualizes battlespace in a variety of domains. The traditional realms of land, air,

[5] Melissa and Michelle Tusan, "Fault Lines of Loyalty: Kipling's Boer War Conflict/War and the Victorians: Response," *Victorian Studies* 58, no. 2 (Winter, 2016): 314-31.

[6] Swinton, Ernest, "The Defence of Duffer's Drift," Department of Defense FMFRP 12-33, 1989. First published 1904.

[7] Merritt, Braden, "Modern Relevance of the *Defence of Duffer's Drift*," United States Naval Institute. *Proceedings* 132, no. 8 (08, 2006): 64-5.

and sea are the most widely known. These domains are not intended to be examined independently, but rather collectively to understand interdependencies during conflict. Recently, the domains of cyber and space were added to reinforce their importance to modern military operations.[8]

The space domain is highly technical and can be intimidating to the uninitiated. Space operations involve orbital mechanics, communication linkages, relay sites on the ground, and airborne assets.[9] Space operations are replete with the latest technology, but they are not necessarily unique in tactics and strategy. At high levels, space operations succeed in the same manner as any other military force. They must ensure mission readiness while maintaining survivability. Maneuver forces use the term, 'shoot, move, communicate' as a sort of mantra when operating in a battlespace. Space assets are no different. Space focused units must be able to ensure each asset can accomplish its designed mission (shoot), reposition for the next objective (move), and synchronize actions to reinforce unity of effort (communicate). The ways and means that space focused units accomplish this are varied due to the exoatmospheric nature of the mission, but fundamentals are the same.

Although Swinton focused his teaching points on tactical/operational concepts such as fields of fire, points of domination, and unity of effort, a wider examination reveals valuable insights into educating space professionals. Collectively, the lessons in *Duffer's Drift* can be cataloged into three overarching themes applicable to space operations: initiative, operational security, and battlefield positioning. Analyzing each of these themes through the lens of space operations shows how Swinton's novella applies to the space domain and reinforces its value to today's space professionals.

Initiative

Initiative is critical for land operations. In *Duffer's Drift*, this is addressed in two ways. First, the lieutenant delays preparing defenses until the next morning. This decision results in lost time, effort, and opportunity toward establishing a foothold along the river. The result for the British forces is disastrous due to ill preparedness. Although space operations do not involve construction of parapets, they do necessitate defensive protections against an adversary.[10] From a strategic perspective the lesson of initiative (while on the defensive) manifests in assessing enemy capabilities and including countermeasures during the satellite design phase. To support this, coordination between research and development (R&D) professionals and the intelligence community can ensure appropriate threat mitigation capabilities are included in new space assets.[11] For the space community, seizing the initiative means investing in early stages of the R&D cycle, so officers never have to wait until after experiencing catastrophe to develop new countermeasures.

A second example comes later in the story when the lieutenant and his men fail to exploit an opportunity to strike first. The enemy is at first unaware of British positions, and an initial volley of rifle fire could turn the battle in the defenders' favor. Yet, the lieutenant

[8] Behling, Thomas G., "Ensuring a Stable Space Domain for the 21st Century," *Joint Force Quarterly* no. 47 (Fourth, 2007): 105-8.

[9] Department of Defense, JP 3-14 Space Operations, Washington, D.C., April 2018.

[10] Hamre, John, "Challenges We Face in the National Security Space Domain," *Hampton Roads International Security Quarterly* (Feb 19, 2017): 14.

[11] Sharma, Surinder Paul, "U.S. Government Program Managers' Competencies to Manage Satellite Acquisition Programs," Order No. 10603364, Northcentral University, 2017.

does not give the order. An opportunity to seize the initiative is lost, and disaster ensues. While U.S. space assets are not yet equipped with strike capability, a linkage to the lesson on initial fires still applies: allocating satellites at the earliest point of sufficient information.

Space capabilities are primarily an enabling function for other domains. Whether providing positioning/navigation/timing services, relaying critical communications, remote sensing, or other functions, satellites require a great deal of planning and coordination.[12] The lesson from *Duffer's Drift*, then, is to identify and prepare assets at the earliest possible point of oncoming conflict. By rapidly taking action, the space community can ensure appropriate platforms are available when needed, enabling those first, highly effective, initial fires from other domains.

Operational Security

A clear example from *Duffer's Drift* of an operational security lesson involves a local trader. The trader seeks an opportunity to sell his wares to the British soldiers. The lieutenant not only allows this man to trade, but he lets him bring his items into camp. It is only when this dream series is complete that the lieutenant realizes his mistake. The trader has reported the location of the camp, its internal defenses, strength of the British compliment, weapons available, and other forms of valuable information to the enemy commander. Undetected, the lieutenant let a spy into camp. The lesson here is one which applies not only to space operations, but to any field or industry, be wary of who, regardless of uniform, has access to sensitive information.

Space operations dazzle with high technology satellites and large launch vehicles, but the central node of any organization is always people. Monitoring who has access to sensitive sites and plans is a requirement for any leader. Swinton's lesson for space professionals can be expanded to include network access, information sharing, operations planning, asset capabilities, and much more. This is especially important in today's globalized society. Meeting the multitude of threats across the globe requires partnership and cooperation.[13] It is imperative to balance the good faith effort of cooperating with multinational coalitions against the priority of ensuring security protocols for protecting space capabilities.

Battlefield Positioning

The story of *Duffer's Drift* is a defensive one. The lieutenant is charged to *defend* terrain with a small force against a potentially larger enemy. Tactics in this type of operation are different from an assault or raid. Solid defense relies on being able to withstand overwhelming firepower. In each dream from the story—except the last—British forces, despite their previous training, succumb to enemy violence. Many of the lessons in Swinton's tale, then, focus on how to defend properly and ensure that each soldier is best able to survive the fight. In the story, ultimate success is accomplished through optimal positioning of forces. Terrain dictates much of the defense, and issues such as dead space in fields of fire, proximity to enemy front lines, and spacing of men are all examined in detail.

Of particular relevance to space operations is a lesson addressing flanking. In the story, the lieutenant and his men lose control of the battle. The enemy maneuvers forces to the

[12] Goirigolzarri, Benjamin L., "A Need for Speed? Identifying the Effects of Space Acquisition Timelines on Space Deterrence and Conflict Outcomes," Order No. 27541013, Pardee RAND Graduate School, 2019.

[13] Moller, Sara Bjerg, "Fighting Friends: Institutional Cooperation and Military Effectiveness in Multinational War," Order No. 10099567, Columbia University, 2016.

flanks of British defenses. Chaos ensues as the lieutenant's men receive hostile fire from multiple angles. Lack of protection on the flanks along with inadequate planning for that scenario results in yet another massacre at the hands of the enemy. Once again, the lieutenant is forced to analyze in detail how he failed. Protecting a flank is, of course, a basic consideration for any ground officer. Maritime and air components are concerned about this threat as well. Space is no different.

Although space is big, it is also, in terms of competitive interactions, crowded. There are multiple actors, both government and private, operating in space.[14] There is an obvious terrestrial threat from ground-launched antisatellite weapon systems, but that is not the only front. In fact, where orbital assets are concerned, the "front," and by implication vulnerable flanks, are everywhere. Space professionals should keep this lesson in mind when planning operations. Kinetic attacks from the planet are not the only way to defeat an orbital asset. Attacks can come from the digital realm in the form of cyber. Laser technology has developed and diffused rapidly, and as a result it can interfere with satellite operations from multiple directions. Jamming signals along an entire spectrum are another threat from either ground or space-based assets.[15] The architecture of space operations is expanding so fast that every conceivable attack vector can be considered a satellite or constellation "flank."

AN OVERARCHING LESSON

Tucked between the pages of Swinton's novella are additional lessons for use in professional development. Each is clearly explained after the dream sequence and incorporated into the next defense. In addition, *Duffer's Drift* provides *general* guidance that is less explicit. These lessons and guides apply to every field regardless of service and can be incorporated in every leader's approach.

The novella, for example, implies the lieutenant is fresh out of military education and training. He is depicted as determined to use his recently acquired knowledge to the fullest extent possible. Yet, it is clear the lieutenant is flummoxed when his training does not provide direct, formulaic solutions for his mission. To reinforce the idea, Swinton includes this quote, "*Now if they had given me a job like fighting the Battle of Waterloo…or Bull Run, I knew all about that, as I had crammed it up....*"

Although critical for the narrative and used to underscore the lieutenant's irritation in the moment, there are deeper lessons to be drawn. First, knowing military history and gaming the intricacies of simulated battles does not guarantee success. Studying a variety of tactical, operational, and strategic actions in any battle scenario helps tell that conflict's story; however, those solutions are guaranteed only to those battles. Each war has its unique aspects, variables, and constraints, limiting the reach of military science. The lesson Swinton is explaining with this quote is to work the problem of the current fight, recognizing it has its own set of variables, not just fresh parameters in the same old formula. It is still important to appreciate the historical record or summary statistics from thousands of simulation runs, but these can never be useful unless officers retain their skepticism: at some point the record will fall short since it cannot emulate actual fighting conditions.

[14] Morin, Jamie, "Four Steps to Global Management of Space Traffic," *Nature* 567, no. 7746 (Mar 07, 2019): 25-7.

[15] Johnson-Freese, Joan, *Space Warfare in the 21st Century: Arming the Heavens*, Taylor & Francis Group, 2016.

The lesson is especially important for today's fledgling space community. The U.S. Space Force is [*sic*] shy of its first birthday, but it claims mature strategic importance with direct representation on the Joint Chiefs of Staff.[16] Its presence on this august council emphasizes the growing role of space capabilities in U.S. strategic thinking. Prior to the creation of USSF, space activities were dispersed throughout the services. Each branch of the military held its own space interests and operations.[17] The U.S. Air Force (USAF) was the largest contingent with a variety of units and roles related to space falling under its mission. As such, the military space community, always a joint venture, was nonetheless dominated by USAF operations and culture.

Naturally, USSF will bring much of this culture and business process to its new service, which remains within the Department of the Air Force. However, the independent JCS seat signals USSF will not be a simple extension of the Air Force.[18] Space Force faces qualitatively new challenges and will be compelled to develop its own approaches to frame and solve these military problems. The deep well of USAF business practices combined with collective experience of the partner services will support USSF as it evolves. Still, it is crucial for this new organization to balance legacy processes with tailored solutions in the midst of unrelenting operations tempo.

The pensive lieutenant facing a novel challenge at *Duffer's Drift*, through his dreaming (that can be read as gaming) applied his imagination to expand his real-life chronological hours for iteration and refinement of traditional tactics. Likewise, USSF relative to older branches ought to leave its door unusually open to investment in the demanding legwork of testing new ideas and radical concepts even as it professionalizes the service.

In the years since Swinton's story was published, a great many aspects of warfare have changed, of course. Weapons are deadlier. Communication has increased in speed and volume. Points on the globe are closer due to faster means of transportation. Access to space for the United States has become a routine expectation. These advances obscure but do not undermine the validity of Swinton's lessons. If anything, they make them more urgent. Space is not yet weaponized, but it must be considered in the context of military operations, subject to analysis through the lens of geopolitical conflict. Swinton's classic story of a young lieutenant faced with a complex, evolving mission can serve as a contemporary tool for space professionals, an early guide to how they can defend this critical domain.

[16] Opening Statement by Ranking Member Reed at SASC Hearing to Hear Proposal to Establish a United States Space Force, Washington: Federal Information & News Dispatch, LLC, 2019.

[17] Tyler, Coley D., "Demystifying Space: How to Perform Better in the Space Domain," *Infantry* (Online) 107, no. 4 (Oct. 2018): 16-9.

[18] Opening Statement by Ranking Member Reed at SASC Hearing to Hear Proposal to Establish a United States Space Force, Washington: Federal Information & News Dispatch, LLC, 2019.

Article

Deterrence in Cyberspace: A Game-Theoretic Approach

Abderrahmane Sokri

This novel application of the Stackelberg leader-follower game from economic theory illuminates situational constraints that point to a sweet spot, an optimal level of investment in cyber defense, for deterrence by denial.

Deterrence is a form of persuasion intended to manipulate the cost-benefit analysis of would-be attackers and convince them that the cost of taking an action against the defender outweighs its potential benefit (Brantly, 2018; Wilner, 2017).[1] It is the prevention (of a target) from committing unwanted behavior by fear of the consequences (United States (US) Department of Defense (DoD), 2008; Taipale, 2010). Deterrence differs from compellence by focusing on prevention using *ex ante* actions. Compellence uses power to force an adversary, *post hoc*, to take a desired action under threat of possible escalation in the future (Brantly, 2018).

Two types of deterrence are generally used: deterrence by punishment and deterrence by denial. Deterrence by punishment hinges on the threat of retaliation against a potential attacker. This tit-for-tat or equivalent retaliation strategy adds to the attacker's perceived cost. Deterrence by denial sends a signal to potential challengers that they will be unsuccessful. This impenetrability strategy subtracts from the attacker's perceived benefits.

In the physical world, deterrence aims to dissuade specific actions against physical assets. In this space, the most common form of deterrence by punishment is the use of nuclear weapons. These weapons are inherently an existential threat against potential challengers (Brodie et al., 1946; Brantly, 2018). An all-out nuclear war could be threatened but never fought to achieve reasonable political objectives (Freedman, 2004; Brantly, 2018). Deterrence by denial may include tightening defense around a critical infrastructure to deny attacker access. The target can be tightly defended by installing, for example, more security mechanisms and higher walls.

In the cyber domain, deterrence is more complex than in the physical domain. Digital attacks go beyond geographic and political boundaries. They are generally highly dynamic and imperceptible to the human senses (Moisan and Gonzalez, 2017; Sokri, 2019b). A cyber-attack may result in interception, degradation, modification, interruption, fabrication, or unauthorized use of an information asset. The information asset can be physically (e.g., hardware) or logically (e.g., software) based (Sokri, 2019a).

Cyber-attacks can be segregated into two main categories: targeted attack and opportunistic attack. A targeted attack requires a large effort and has the potential to cause significant damage to the defender. Denial of service and theft of information are typical targeted attacks. In contrast, an opportunistic attack has a number of intermediate targets, requires a small effort, and tends to cause less damage. A virus and spam e-mail are typical opportunistic attacks.

[1] Abderrahmane Sokri is data scientist at Defence Research and Development Canada, Center for Operational Research and Analysis. Copyright for this article remains with the Crown, Canada.

The most challenging problem in cyber deterrence is the attribution dilemma (Wilner, 2017). Determining who to blame for an attack may be very difficult and time-consuming to do. Consequently, the credibility of any deterrence by punishment in digital space will depend on the blame attribution. (Glaser, 2011; Brantly, 2018). Since deterrence by denial does not require identification of potential attackers, it can be used to mitigate this dependency (Bordelon, 2016).

Cyber risk is present when a given threat meets a vulnerability in an information system allowing it to manifest. In this context, a threat is a potential cause of an unwanted occurrence while a vulnerability is a weakness in the information system (Sokri, 2019a; Zhang, 2012; Bowen et al., 2006). To minimize digital risk against an information asset, the defender should know at least two elements: (1) the probability of a successful attack and (2) the corresponding potential loss (Brantly, 2018; Glaser, 2011; Schneidewind, 2011; Branagan, 2012).

To protect their information assets against offensive cyber-attacks, policy makers are increasingly gravitating towards deterrence by denial (Taipale, 2010). A key decision-variable in digital deterrence by denial is the defender investment level in security. To protect a potential target, the defender can reduce the probability of a successful attack by investing in information security. The investment may, for example, reduce the vulnerability of the target.

The aim of this paper is to show how deterrence by denial as a defense strategy can be formulated in cyberspace using a sequential game with a disclosure mechanism. It shows the suitability of game theory to cyber deterrence. The paper extends existing models by providing a new game formulation of deterrence using a more intuitive probability of a successful attack. It also combines stochastic simulation and game-theoretic approaches to handle uncertainty in the input data. A simulation could, for example, incorporate uncertainty on the model variables and parameters by changing their static values to statistical distributions.

Consider a sequential security game played between two adversarial agents: a defender *D* (the leader) and a strategic attacker *A* (the follower). The defender anticipates the attacker’s reaction, determines, and credibly communicates the security investment to protect an information system. The defender can, for example, publicly release his level of investment in (1) detection and prevention techniques such as Antivirus software, Firewalls, and Intrusion Detection Systems (IDS) and (2) physical monitoring and inspection procedures (Sokri, 2019b). Revenue agencies usually use this tactic by revealing their auditing strategies to deter tax evasion (Cavusoglu et al., 2008).

The attacker observes the defender’s decision and reacts with a certain level of willingness-to-attack. The true willingness-to-attack is latent and, therefore, not directly observable. It is modeled as the expected effort to be exerted by the attacker to compromise the system. The attacker’s effort corresponds to the first activities of the cyber kill chain (Mihai et al., 2014). These activities particularly include (but are not limited to):

1. **Reconnaissance** – the process of collecting information about the system,
2. **Weaponization** – the process of analyzing the collected data to select the appropriate attack technique, and
3. **Delivery** – the process of transmitting the weapon to the targeted system.

Following this introduction, section 2, below, provides a comprehensive review of literature on security investment as a deterrence factor. Section 3, sets up a new game theoretic model of deterrence in cyberspace. Section 4, computes the Stackelberg equilibrium. Section 5 offers a formal discussion about the main results. Some concluding remarks are indicated in section 6.

LITERATURE REVIEW

Identifying and understanding the factors influencing the decision to invest in information security is a key requirement for any effective deterrence and risk management in cyberspace. These factors form the pillars of the appropriate level of security investment. Security investment as a deterrence factor has been an active research area in the last decade. This literature can be divided into two main categories: decision theory and game theory approaches (Cavusoglu et al., 2008).

The decision-theoretic approach uses traditional risk analysis and cost–benefit perspectives for security investment decisions. This approach assesses the risk associated with security breaches and conducts a cost-benefit analysis to determine a certain level of security investment to mitigate the risk. While this approach can assess the economic value of intangible costs and benefits, it has two main limitations: (1) It does not determine the optimal security investment level. (2) It does not allow a defender's security investment to influence the attacker's behaviour.

Al-Humaigani and Dunn (2003), for example, proposed a model to quantify the return on security investment (ROSI). The authors enumerated the fundamental components of ROSI for every organization and security threat. They included what it costs to invest in information security spending (e.g., the cost of procuring the security tool or software, the losses in reputation and goodwill). They incorporated both the pre- and post- system implementation security measures.

In order to come through the first limitation of the decision-theoretic approach, Gordon and Loeb (2002) presented an economic model that determines the optimal amount to invest in information security. Their results indicate that defenders may be better off concentrating their efforts on information assets with midrange vulnerabilities. Extremely vulnerable information assets may be very expensive to protect. For some broad classes of security breach probability functions, results also indicate that optimal investment never exceeds 37% of the expected loss. Hausken (2006) examined the effect of different returns assumptions on the optimal level of investment. The author showed that optimal investment level may no longer be capped at 37% of expected loss. For an alternative class of security breach probability functions, the optimal investment can increase convexly in vulnerability and exceed 37%.

More recently, Mayadunne and Park (2016) used the expected utility approach to analyze information security investment decisions. They provided a comparison between the decisions made by a risk taking and a risk neutral decision maker. They found, for example, that for a group of information assets with equal value and varying vulnerabilities, the risk neutral decision maker will diversify security investment to a greater extent and the risk taker will invest a larger amount when protecting the high risk assets in the group.

The game-theoretical approach uses game oriented models to capture the strategic interactions between rational attackers and defenders. Optimal investment in security is one of the defenders' resulting strategies. This approach has two main challenges: (1) Validity of the game-theoretic assumptions in cyberspace (e.g., rationality of players). (2) Complexity of the cyber domain scenarios (e.g., dynamic attacks and complex networks).

Cavusoglu et al. (2008), for example, argued that the old decision-theoretic approach is incomplete because it does not take into account the strategic nature of the interaction between attackers and defenders. The authors used a game-theoretic model to determine the optimal security investment level. Results indicate that the defender generally enjoys a higher payoff than that in the decision theory approach. The gap between the two results decreases over time and the rate of convergence depends on the defender learning model.

Wu et al. (2015) used game theory to model the relationship between the optimal information security investment and the characteristics of defenders' security environment. Results indicate that defenders are better off not investing in security (outside best practices) until the potential loss reaches a certain value. They should focus on the midrange of intrinsic vulnerabilities. When the potential loss is catastrophic, they should adopt other measures and stop investing in security.

More recently, Pan et al. (2017) suggested an optimal investment strategy using a game-theoretic framework. The authors concluded that the defender is better off using a single security level to protect all the information assets instead of using different security levels to protect different assets. The interested reader is referred to Sokri (2019a) and Sokri (2019b) for further information on game theory in cyber defense.

A "STACKELBERG" DETERRENCE MODEL

The system is characterized by an inherent vulnerability v_0. Each successful attack can result in a potential loss l to the defender and a possible benefit b to the attacker. The loss/benefit occurring can be tangible (e.g., monetary loss/benefit) or intangible (e.g., loss/gain in reputation).

Probability of a successful attack

Let i be the defender's security investment and t the attacker's level of effort to expend in hacking the defender. The compound probability p of a successful attack can be expressed as the product of the probability that the vulnerability may be exploited, $v(i)$, and the threat probability (i.e., the probability to receive an attack) (Wu et al, 2015):

$$(1) \quad p = v(i)\left(1 - exp\left(-\frac{t}{\mu}\right)\right),$$

where the expected effort t can be expressed in terms of time. The threat probability, also known as the probability of attack (prior to information about target vulnerability), is written in Equation 1 as the cumulative distribution function (CDF) of an exponentially distributed random variable evaluated at t. This CDF estimates the probability that the attacker's level of effort will be less than t. The parameter μ represents the mean effort to attack (e.g., investigation, identification, weaponization done prior to knowledge of target defenses). It also represents the standard deviation of the distribution.

As in Wu et al. (2015), the defender's security investment does not directly affect the inherent threat probability. The defender can only reduce the first term, probability that the vulnerability may be exploited, using security investment i. That is,

(2) $v(i) = v_0 \exp(-\alpha i)$,

where the parameter $\alpha > 0$. Straightforward derivation leads to

(3) $\frac{v'(i)}{v(i)} = -\alpha$,

which means that the parameter α is the decay rate of the probability that the vulnerability may be exploited. It represents the rate at which vulnerability decreases with investment in cybersecurity. It can also be seen as a measure of investment productivity. It measures how efficiently security investment is used to reduce the asset vulnerability.

One can also readily see that $v(i)$ satisfies the following three assumptions.

- Assumption 1. $v(0) = v_0$.
- Assumption 2. $\lim_{i \to \infty} v(i) = 0$.
- Assumption 3. $v'(i) = \frac{dv(i)}{di} < 0$, $v''(i) = \frac{d^2 v(i)}{di^2} > 0, \forall i$.

Assumption 1 states that if there is no investment in security, the vulnerability of the system will be the inherent vulnerability. Assumption 2 states that no finite investment can eradicate the vulnerability from information systems. Because of their complexity, perfect security is impossible (Wu et al., 2015). Assumption 3 states that the investment in security reduces the probability that the vulnerability may be exploited, but at a decreasing rate. Investment makes the system more secure, but with declining marginal return.

The probability of vulnerability exploitation is formulated in Equation 2 as an exponentially decreasing function of the security investment. Consequently, the probability of a *successful* attack can now be written as

(4)

$$p(i,t) = v_0 \exp(-\alpha i)\left(1 - \exp\left(-\frac{t}{\mu}\right)\right).$$

This probability depends on the defender investment level and the attacker's effort level, in addition to the system's inherent vulnerability.

Defender's loss and attacker's payoff

In this game the defender seeks to find the optimal security investment that minimizes the following total cost

(5) $W_D = p(i,t)l + i$,

where the first term of its right-hand side is the defender's expected loss due to a successful attack. The attacker seeks to maximize the following payoff

(6) $W_A = p(i,t)b - t$,

where the first term of the right-hand side is the attacker's expected benefit and the second term represents the expected effort to compromise the system.

Deterrence game's equilibrium

This section characterizes the optimal solution to the deterrence game. As in the standard Stackelberg competition, the game is sequential: the defender moves first, committing to a strategy before the attacker reacts. The defender's strategic choice is to select the optimal security investment (deterrence by denial). The attacker's choice is to determine his appropriate level of effort. The outcome of this leader-follower interaction is called Stackelberg equilibrium. This equilibrium has been recognized as a sound theoretical framework for modeling the strategic interactions between attackers and defenders (Jain et al., 2010; Korzhyk et al., 2011; Kiekintveld et al., 2015; Acquaviva, 2017).

Proposition 1. The following condition is satisfied at equilibrium

(7) $\frac{\partial p(i,t)}{\partial t} b = -\frac{\partial p(i,t)}{\partial i} l.$

Proof. Assuming an interior solution, the first-order condition (maximizing attacker payoff with respect to effort, *t*) for the attacker optimization problem is

(8) $\frac{dW_A}{dt} = \frac{\partial p(i,t)}{\partial t} b - 1 = 0.$

The optimality condition for the defender problem is

(9) $\frac{dW_D}{di} = \frac{\partial p(i,t)}{\partial i} l + 1 = 0.$

Equations 8 and 9 lead to the equilibrium condition in the Proposition.

■

Fixing the defender's security investment to some strategy i, the first problem to be solved is to find the attacker's best response to i. In this optimization problem, the follower maximizes his expected benefit given i.

Proposition 2. Assuming an interior solution, the optimal effort the attacker is willing to exert is given by

(10) $t = -\alpha\mu i + \mu \ln\left(\frac{bv_0}{\mu}\right)$

Proof. After substitution for $p(i,t)$, Equation 6 becomes

(11)
$W_A = v_0 \exp(-\alpha i)\left(1 - \exp\left(-\frac{t}{\mu}\right)\right) b - t.$

Computing the derivative of W_A with respect to t, equating to zero, and solving leads to the expression of t as a function of i.

■

Proposition 3. The attacker's level of effort is a decreasing function in the defender's investment.

Proof. The derivative of *t* with respect to *i* is

(12) $\frac{dt}{di} = -\alpha\mu < 0.$

■

Proposition 4. Assuming an interior solution, the defender optimal security investment level is given by

(13) $i = \frac{1}{\alpha}\ln(\alpha l v_0).$

Proof. Equations 4 and 5 imply that

(14)
$W_D = v_0 \exp(-\alpha i)\left(1 - \exp\left(-\frac{t}{\mu}\right)\right) l + i.$

The expression of t in Equation (10) is equivalent to

(15) $\exp\left(-\frac{t}{\mu}\right) = \frac{\mu}{bv_0}\exp(\alpha i).$

Substituting for $\exp\left(-\frac{t}{\mu}\right)$ from Equation 15 in Equation 14, computing the derivative of W_D with respect to i, equating to zero, and solving provides the equilibrium strategy in the Proposition.

■

Proposition 5. The attacker's optimal level of effort is given by

(16) $t = \mu \ln\left(\frac{b}{\alpha\mu l}\right).$

Proof. Substituting for i from Equation 13 in Equation 10 leads to the result.

■

Proposition 6. The defender should not invest in security beyond best practices until the potential loss reaches

(17) $l^* = \frac{1}{\alpha v_0}.$

Proof. To have a positive investment, $\ln(\alpha l v_0) > 0$. This is possible only if $\alpha l v_0 > 1$, which leads to the condition in the Proposition.

■

Proposition 7. The attacker should not exert any effort until the potential benefit reaches

(18) $b^* = \alpha \mu l.$

Proof. To have a positive effort, $\ln\left(\frac{b}{\alpha \mu l}\right) > 0$. This is possible only if $\frac{b}{\alpha \mu l} > 1$ which leads to the condition in the Proposition.

■

Proposition 8. The defender's optimal security investment level is an increasing concave function of the potential loss, l.

Proof. As shown in Equations 19 and 20, the first derivative of i with respect to l is positive and the second derivative is negative, respectively.

(19) $i'(l) = \frac{di(l)}{dl} = \frac{1}{\alpha l} > 0.$

(20) $i''(l) = \frac{d^2 i(l)}{dl^2} = -\frac{1}{\alpha l^2} < 0.$

Consequently, i is a concave function in l that increases at decreasing rate.

■

Proposition 9. The defender's optimal investment spent on information security as a fraction of potential loss l is given by

(21) $r(l) = \frac{i}{l} = \frac{1}{\alpha l}\ln(\alpha l v_0).$

Proof. Dividing the expression of i in Equation 13 by l leads to the result.

Proposition 10. The fraction $r(l)$ is an increasing function in the potential loss l for $l \leq l^{**} = \frac{e}{\alpha v_0} \approx \frac{2.718}{\alpha v_0}$. It is decreasing for $l \geq l^{**}$ with a horizontal asymptote at $y = 0$.

Proof. The first derivative of $r(l)$ with respect to l is

(22) $r'(l) = \frac{dr(l)}{dl} = \frac{1}{\alpha l^2}\left(1 - \ln(\alpha l v_0)\right).$

It is straightforward to show that
$r'(l) = 0$ for $l = \frac{e}{\alpha v_0}$, $r'(l) \geq 0$, for $l \leq \frac{e}{\alpha v_0}$, and $r'(l) \leq 0$, for $l \geq \frac{e}{\alpha v_0}$.
Hence, the potential loss l that maximizes the fraction $r(l)$ is given by

(23) $l^{**} = \frac{e}{\alpha v_0} \approx \frac{2.718}{\alpha v_0}.$

Using the l'Hopital rule, $\lim_{l \to \infty} r(l) = 0$, which shows that $r(l)$ has a horizontal asymptote at $y = 0$.

■

To deal with uncertainty in the input data, a Monte Carlo simulation could represent each uncertain parameter as a probability distribution.

INVESTMENT IN CYBERSECURITY AT EQUILIBRIUM

A parsimonious game-theoretical model is used in this paper to characterize deterrence in cyberspace. A Stackelberg game is played to capture the strategic nature of this interaction and provide clear insights about it. The suggested mechanism involves disclosing the defender's investment information to the potential attacker. The game's logic and results crucially depend on the timings of each move. The defender moves first, anticipates the strategic behavior of the attacker, and decides on the security investment. The attacker observes the defender's level of investment and determines a certain effort level. By revealing the security investment strategy, the defender becomes able to control the attacker's incentive and deter (or reduce the effort behind) potential attacks.

Assuming an interior solution, Proposition 1 characterizes the first-order optimality conditions for the defender and attacker strategies. It compares, at equilibrium, magnitude decline in expected defender loss from extra security investment to magnitude increase in expected attacker benefit from extra effort. Stackelberg interaction joins their fates.

At equilibrium, marginal reduction in defender's expected loss due to additional investment precisely balances marginal increase in the attacker's expected benefit attributable to additional effort. In order to reach this decision point, the attacker as follower must be able to measure the magnitude of loss to the defender from a successful cyber attack. In the Stackelberg interaction, attacker does have a clue from observing optimal defender security investment, which is tied to defender assessment of cost in the event of disruption. Physical properties of the cyber system's vulnerability must also be common knowledge.

Propositions 4 and 5 define the attacker's optimal level of effort and the defender's optimal investment, respectively. Proposition 4 relates the defender's strategy to three parameters:

- the inherent vulnerability v_0
- the decay rate in the vulnerability due to investment α, and
- the defender's potential loss l.

Proposition 5 shows that the attacker's strategy depends on two other parameters in addition to α and l, namely the mean level of effort μ (independent of system vulnerability) and the attacker potential benefit b from system disruption.

The derivative of the attacker's expected effort t with respect to the defender's investment i in Equation 12 indicates that the parameters α and μ and their interaction effect are the key factors in cyber deterrence, that is, in sharply affecting adversaries' attack plans through denial. Equation 12 shows that the higher the two parameters the more likely the attacker is to be deterred through additional defender investment. The parameter α measures the speed at which security investment translates into a reduction of the asset's vulnerability to attacks. An increase in the parameter α for any given level of investment will decrease the probability that inherent vulnerability may be exploited, lessen the probability of a successful attack, and, therefore, result in a reduction in the attacker's level of effort. At the same time, the influence of additional investment on reducing attacker effort even further will rise. Equation 12 also shows that opportunistic attacks (with small μ) are harder to influence than targeted attacks (with high μ). Extensive initial interest in the targeted system leads potential attackers to be discouraged at a steeper rate once they learn of additional defender investment.

Propositions 6, 8 and 9 characterize the defender's optimal security investment level i as a function of the potential loss l. These propositions highlight the following key findings:

- The defender should not invest in security beyond best practices until the potential loss reaches a given value;
- The optimal security investment increases with the expected loss at a decreasing rate;
- The optimal investment in security as a fraction of potential loss l has a horizontal asymptote at $y = 0$. This means that, for very large potential losses, the optimal amount to spend on information security does not keep

pace; it is far smaller than the potential loss.

These findings are on par with the deterrence literature. They are particularly consistent with the study conducted by Gordon and Loeb (2002).

The formalism in Equations 4, 5, and 6 is grounded theoretically such that the model could be repeated or extended using different probability distributions. Its underlying mathematics is clear and conceptually based. Variations of the probability distribution will provide qualitatively the same findings. The numerical values of these findings will, of course, depend on the values of the deterrence model parameters.

A myopic approach such as a simultaneous game or a decision-theoretic technique would produce different results. Under a simultaneous game, players make single decisions before seeing the other player's moves (as in the famous Prisoner's Dilemma [PD]) and possibly under incomplete information about the other player's payoff from certain outcomes. Attackers, for example, are not able to observe the outcome of previous actions before responding. The main characteristic of myopic approaches is the non-cooperative, monotonic relationship between defender investment level and attacker effort. Both players rationally defect in PD-type games. When one cost variable increases, the other increases and vice versa; net payoffs in equilibrium for both decline. In this situation, attackers are never deterred, *per se*, because myopic approaches lack disclosure mechanisms. A deeper understanding of this interaction will be generated in future works.

CONCLUSION

Deterrence is used to prevent unwanted actions by influencing the cost-benefit analysis of potential attackers. The most common form of deterrence in cyberspace is deterrence by denial. Deterrence by denial sends a signal to would-be attackers that they will be unsuccessful. In this defense strategy, the defender reduces the probability of a successful attack by investing in information security. While the credibility of deterrence by punishment depends on blame attribution, deterrence by denial does not require this knowledge.

This paper used a sequential game theoretic approach with a disclosure mechanism (Stackelberg competition) to formulate a deterrence strategy in cyberspace. It derived the defender's optimal security investment level and the attacker's level of effort. The factors influencing the decision to invest in cybersecurity were identified and discussed. To deal with uncertainty in the input data, the model invites parametric analysis using Monte Carlo simulation.

Results for the equilibrium indicate that effectiveness of the security investment (α) and the category of attack (μ) and their interaction effect are the key factors in cyber deterrence. The more effective the security investment in reducing vulnerability and the higher attacker initial interest in the target, the more likely attacker is to be deterred by additional investment. Targeted attacks aiming at significant damage to the defender are more manageable by security investment than opportunistic attacks.

The defender's optimal security investment level (i) as a function of potential loss (l) indicates that investment in cybersecurity as a deterrence strategy will top out after the middle part of losses. At very high levels of loss, there is a numbing effect; optimal investment does not change much with additional increments of loss.

Deterrence in the cyber domain is more complex than in the physical field. Further efforts should be undertaken to understand it in order to influence potential attackers' behaviors. Examples of such studies include (but are not limited to)

- application of the model to a real-world cyber-security problem using real-life parameters,
- analyzing the interaction between defenders and attackers in dynamic scenarios,
- assessing the risk to the defender of a disclosure strategy,
- including deception mechanisms to enhance security,
- developing models to deal with bounded rationality of human adversaries,
- combining game theoretic models such as this Stackelberg version with other techniques and tools to make the formalism more realistic and tractable; techniques may include numerical simulation and genetic algorithms; tools may consist of firewalls and anti-virus software.

REFERENCES

Al-Humaigani, M., and Dunn, D. (2003). A model of return on investment for information systems security. IEEE 46th Midwest Symposium on Circuits and Systems, Vol. 1, pp. 483-485.

Acquaviva JR (2017). Optimal Cyber-Defence Strategies for Advanced Persistent Threats: A Game Theoretical Analysis. Master Thesis, the Pennsylvania State University.

Bordelon, E.B. (2017). Approaching Cyber Warfare: Geopolitics, Deterrence, and International Law. Senior Honors Thesis 639, Cyber War and Geopolitcs, Liberty University, Virginia.

Bowen, P., Hash, J., and Wilson, M. (2006). *Information Security Handbook: A Guide for Managers*. National Institute of Standards and Technology (NIST) Special Publication 800-100.

Branagan, M. (2012) A risk simulation framework for information infrastructure protection. Ph.D. Dissertation, Queensland University of Technology, Australia.

Brantly, A.F. (2018). The cyber deterrence problem. 10th International Conference on Cyber Conflict (CyCon), IEEE, pp. 31-54.

Cavusoglu, H., Raghunathan, S., and Yue, W.T. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, Vol. 25:2, pp. 281-304.

Freedman, L. (2004). *Deterrence*. Polity Press, Cambridge.

Glaser, C.L. (2011). Deterrence of Cyber-attacks and US National Security. Report GW-CSPRI-2011-5, The George Washington University, Washington, D.C.

Gordon, L. A., and Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security* (TISSEC), Vol. 5:4, pp. 438-457.

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers*, Vol. 8:5, pp. 338-349.

Jain M, Tsai J, Pita J, Kiekintveld C, Rathi S, Ordone, F, and Tambe, M. (2010). Software assistants for randomized patrol planning for the LAX airport police and the Federal Air Marshals Service. *Interfaces*, Vol. 40:4.

Kiekintveld C, Lisy V, and Pibil R. (2015). Game-theoretic foundations for the strategic use of honeypots in network security. In *Cyber Warfare*. Springer, p. 81–101.

Korzhyk D, Yin Z, Kiekintveld C, Conitzer V, and Tambe M. (2011). Stackelberg vs. Nash in

Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness. *Journal of Artificial Intelligence Research*, Vol. 41.

Mayadunne, S., and Park, S. (2016). An economic model to evaluate information security investment of risk-taking small and medium enterprises. *International Journal of Production Economics*, Vol. 182, pp. 519-530.

Mihai, I.C., Pruna, S. and Barbu, I.D. (2014). Cyber Kill Chain Analysis. *Int'l J. Info. Sec. & Cybercrime*, Vol. 3.

Moisan, F. and Gonzalpez, C. (2017). Security under Uncertainty: Adaptive Attackers Are More Challenging to Human Defenders than Random Attackers. *Frontiers in Psychology*, Vol. 8:982.

Pan, C., Zhong, W., and Mei, S. E. (2017). Investment strategy analysis of information systems with different security levels. IEEE 2nd International Conference on Big Data Analysis, pp. 703-708.

Pereira, J. P., & Ferreira, P. (2011). Next Generation Access Networks (NGANs) and the geographical segmentation of markets. ICN Tenth International Conference on Networks, pp. 69-74.

Schneidewind, N.F. (2009). *Systems and Software Engineering with Applications*. Wiley-IEEE Press.

Sokri, A. (2019a). Cyber Security Risk Modelling and Assessment: A Quantitative Approach. Proceedings of the 19th European Conference on Cyberwarfare and Security (ECCWS19), 4-5 July 2019, Coimbra University, Portugal.

Sokri, A. (2019b). Game theory and cyber defence. In: *Games in Management Sciences*, Pineau, P.-O. and Taboubi, S. (eds) Springer International Series in Operations Research & Management Science.

Taipale, K.A. (2010). Cyber-deterrence. Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization, IGI Global.

US DoD (2008). Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, Washington, D.C.

Wilner, A. (2017). Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Comparative Strategy*, Vol. 36:4, pp. 309-318.

Wu, Y., Feng, G., Wang, N., and Liang, H. (2015). Game of information security investment: Impact of attack types and network vulnerability. *Expert Systems with Applications*, Vol. 42:15-16, pp. 6132-6146.

Zhang, J. (2012). Information Security Risk Management Framework: China Aerospace Systems Engineering Corporation. Master Thesis, University of South Australia.

Cadet Voice
Artificial Intelligence and Stability in Nuclear Crises

Marshall D. Foster

The following USAFA cadet independent study, with the exception of minor grammatical corrections, is produced as presented at the winter conference of the Project on Nuclear Issues (PONI), Center for Strategic and International Studies, Washington, D.C., Dec. 11, 2019 (https://www.csis.org/events/poni-2019-winter-conference).

Technological advances in artificial intelligence (AI) by the United States, China and Russia jeopardize the longstanding nuclear peace that the world has enjoyed since the end of the Cold War.[1] The desire to obtain AI capabilities for the purpose of strengthening defense and security postures could spur a new arms race among these powerful nuclear states, and the United States, China, and Russia have all expressed their interest in extensive AI research and in the implementation of AI in their nuclear operations. The application of AI in the nuclear operations of a superpower risks undermining the world's relatively stable nuclear infrastructure, as AI could essentially make a nuclear war "winnable" for the power that can harness its benefits first. Furthermore, and perhaps more importantly, the likely asymmetric acquisition of AI-enhanced technology will introduce a new degree of uncertainty as these great-power states incorporate it into their nuclear systems. As this uncertainty escalates, nuclear crisis stability may experience severe adverse effects, increasing the chances of a hostile nuclear strike.

This study examines the probable impacts of the asymmetric acquisition of AI-capabilities on nuclear crises stability by defining relevant terms, reviewing relevant existing literature and relevant historical cases, forecasting how asymmetry will affect stability, and formulating a methodology to predict how asymmetry may arise in the future.

Ultimately, it concludes that the likely forthcoming asymmetry will decrease nuclear crisis stability. In response, the United States and the international community should engage in methods to limit the likelihood of great-power states seizing advantages that AI may provide for their nuclear capabilities. These methods include pushing for transparency, intelligence gathering, and arms control.

LITERATURE REVIEW AND RELEVANT DEFINITIONS

Future Impacts of AI

Michael Horowitz's analysis of possible first-mover advantages following AI development has set the stage for research in this field. Horowitz aims to answer the question, "What will advances in artificial intelligence mean for international competition and the balance of power?" (Horowitz, 2018: 37). He evaluates how

[1] Second Lieutenant Marshall Foster (USAFA '20) is pursuing his master's degree at Georgetown University, Washington, D.C.

developing AI capabilities will influence military power and international relations while stressing that AI is more than a technology within itself. Rather, AI is an enabler like electricity or a combustion engine. Answering his original question, Horowitz provides two possible answers.

First, "key drivers of AI development in the private sector could cause the rapid diffusion of military applications of AI, limiting first-mover advantages for innovators" (Ibid.: 37). On the other hand, Horowitz recognizes that the application of AI to military uses may be more difficult than many expect and therefore may provide substantial first-mover advantages for global powers. When comparing these two possibilities, he asserts that diffusion of AI would lower the likelihood of a first-mover advantage, but military AI may be more "excludable" than civilian uses of AI and may generate more first-mover advantages.

Since there is high-cost, up-front research and development for acquiring AI systems that will enable rapid power projection, Horowitz tends to believe that AI will indeed produce significant first-mover military advantages despite private sector diffusions. He states that the integration of AI into early-warning systems and its ability to aid in rapid targeting could also affect crisis stability and nuclear weapons, but he conspicuously does not elaborate on the topic. Recognizing these advantages helps predict outcomes when comparing the asymmetrical abilities of competing states.

Elaborating on the ideas that Horowitz presented, Elsa Kania believes that AI "should be recognized as a strategic technology with implications for national competitiveness that extend well beyond the military domain" (Kania, 2018: 11). States may apply it to a wide range of objectives, including military, economic, and educational programing. As a policy response, Kania suggests that great-power states seek opportunities to cooperate on AI issues and to prevent escalation of AI warfare. For instance, the United Nations Group of Governmental Experts provides one means of accomplishing this goal. The working group brings together over twenty states to engage in conversations regarding state behavior in cyberspace as it enables "vital discussions of core concepts and questions, particularly ethical issues and human control, and hopefully can create a critical foundation for future engagement" (Kania, 2018: 18).

Separately from the intersection of the two technologies, Kania provides an analogy between the rise of AI and that of nuclear weapons. The advent of nuclear weapons posed a similar threat to strategic stability, and during the height of the Cold War and following the collapse of the Soviet Union, nuclear weapons states discussed shared concerns and aversions. Kania believes that similar cooperation and discussion regarding pragmatic measures aimed at risk reduction will be equally beneficial. However, due to the ambiguity concerning formalized definitions of AI and the wide range of AI capabilities, cooperation in this realm may be even more difficult than that for nuclear weapons, and this will require a greater degree of transparency regarding intent and capabilities.

Adding to the conversation, James Johnson discusses the deterministic and dramatic potential effects, from the tactical to the strategic level, that AI will have on military power, strategy, and the global balance. He argues that if "left unchecked, the uncertainties and vulnerabilities created by the rapid proliferation and diffusion of AI could become a major potential source of instability and great power strategic rivalry"

(Johnson, 2019: 148). This is similar to Horowitz's thesis, but Johnson focuses on managing escalation and unique risks of AI rather than first-mover advantages.

Specifically related to nuclear deterrence, Johnson discusses the integration of AI into early-warning systems. This application may accelerate the decision-making process and the stages of the escalation ladder to employ a nuclear attack. In addition, "a state could deploy long-range, offensive conventional missile salvos enhanced by big data analytics, cyber capabilities, and AI-augmented autonomous weapons, and then use its missile defenses to mop-up an adversary's remaining retaliatory capabilities" (Ibid.: 152).

Both of these scenarios could have a negative impact on nuclear crisis stability as they provide conditions that could offer advantages for a state to strike first against an adversary. Furthermore, Johnson holds that states may soon develop AI-augmented weapons systems. These systems, along with AI-enabled early-warning systems and sensors, "could adversely impact the international security and, potentially, crisis stability at a nuclear level of warfare" (Ibid.: 159).

Finally, utilizing scenarios regarding aggression between Russia and NATO, Michael O'Hanlon (2018) illustrates how AI will alter the future of warfare. He discusses the potential for escalation following possible Russian attacks on the Baltic States, which ranges from minimal ground conflicts to nuclear warfare. While O'Hanlon believes there are appropriate measures in place, coming from both NATO and Russian deterrence policies, that will prevent escalation to war on a nuclear level, the introduction of AI could seriously damage this crisis stability. According to O'Hanlon, there is currently a relative balance of tactical [*sic*] capabilities between nuclear weapons states. One country might improve its missile defense capabilities, but an adversary might produce a new nuclear missile with improved agility and speed.

This present balance upholds stability between states, as there cannot likely be a clear winner in a nuclear exchange. Unfortunately, as O'Hanlon argues, the application of AI to military systems undermines this stability for a number of reasons. First, "it seems implausible that arms control agreements [regarding AI] would prevent the development and deployment of… autonomous systems" (O'Hanlon, 2018: 8). States would feel powerful incentives to produce autonomous systems because the mere possibility of another state accomplishing this feat first would place the first at a severe disadvantage.

Second, at present, there is no clear response to an attack made with AI. This dilemma mirrors the cyber realm since an attack that utilizes AI or cyber can come in many different forms and degrees of severity, rendering it difficult for a state to formulate a response that is appropriate and that does not escalate the conflict. Finally, "the degree of difficulty [of winning a war with AI] would be quite considerable and the degree of escalatory risk highly unsettling" (Ibid.: 21). Again, like cyber warfare, AI introduces a high level of ambiguity to conflict since it is not clear what an AI attack will look like or the form it will take.

Stephen Cimbala (2012) presents an argument that is in line with O'Hanlon's. Cimbala holds that the uncertainty that AI will bring to the battlefield will undermine stability. Overall, O'Hanlon's various scenarios revolving around the implementation of AI into military systems effectively demonstrate how AI will affect conflict at the tactical level and how these tactical repercussions alter strategic stability.

The Likely Asymmetric Acquisition of Capabilities

In addition to projecting the impacts of AI, Kania (2018) provides analysis on how the U.S., China, and Russia have embarked on an AI arms race. There is ongoing military competition between these states as they attempt to advance their AI capabilities, and the United States is arguably but likely the current leader. However, China is prioritizing military innovation and actively seeking a wide range of defense applications of AI, placing them as a close second to the United States in this competition. Additionally, Russia's pursuits in the same realm are advancing at a rapid pace. Kania's underlying argument lies in the idea that the term "arms race" is too simplistic to capture the strategic consequences of the AI revolution.

Supporting this claim and building upon Horowitz, Kania states that AI is not a weapon in itself. Rather, AI is a utility that states can utilize to enhance their existing military capabilities. In this sense, AI is more synonymous with electricity or the steam engine than a specific weapons system since it is only useful due to its applications. States cannot launch AI at another state, but they can employ autonomous planes, self-guided nuclear missiles, or various other weapons systems with AI.

Like Kania, Adrian Pecotic (2019) addresses the apparent race for AI between the United States, Russia, and China. However, instead of calling for global cooperation and dialogue as Kania did, Pecotic focuses on different approaches to AI implementation and claims that whichever state successfully incorporates AI into their military systems will secure significant military advantages. He admits that "it's tough to tell what sort of advantage is at stake, because we don't know what sort of thing AI will turn out to be" (Pecotic, 2019: 3). Nonetheless, there will be advantages following the acquisition of AI capabilities, and they may take the form of autonomous drones, more efficient supply changes, or autonomous nuclear missiles.

Additionally, just as Kania predicted, Pecotic believes that advances in AI may resemble the nuclear weapons buildup of the Cold War. He suggests that the main competition will be between the United States and China and does not have the same solution for the situation as Kania provided. Pecotic holds that "once China or the United States is confident in a stable lead [in AI], they will have few incentives to compromise or share technology" (Ibid.: 22).

Defining Crisis Stability

A significant number of scholars and practitioners have spent time defining crisis stability. This study will focus on the definition presented by Thomas Schelling, which has prevailed throughout the evolution of nuclear deterrence literature. As Schelling famously stated, "the reciprocal fear of surprise attack" may drive states to launch a presumptive strike. In this case, "fear that the other may be about to strike in the mistaken belief that [one side is] about to strike gives [this side] a motive for striking, and so justifies the other's motive" (Schelling, 1958: 1).

This scenario describes the essence of crisis stability, which exists when neither side feels the pressure to strike the other out of fear that the other is about to strike. Furthermore, the acquisition of new offensive capabilities threatens crisis stability. As Robert Jervis describes, under circumstances in which a state fears an adversarial attack, "the state's efforts to deter the adversary or protect itself in case of war would make war more likely.

Observing the state's preparations, the adversary would see the danger of war increasing and would itself make ready to strike" (Jervis, 1993: 242).

The introduction of AI into nuclear systems may create the circumstances Jervis describes. As the literature from Horowitz, Kania, and others has demonstrated, AI is a technology enhancer that possesses unknown potential and is clouded with uncertainty. It will be very difficult for states to predict how others will utilize AI, how they will rely on AI, and how they will program their automated machines. Altogether, AI will introduce many unknowns in a state's calculations when predicting an adversarial attack. This uncertainty may create situations in which crisis stability diminishes.

As Glenn Kent and David Thaler describe, crisis *instability* is the "condition that exists when either leader feels pressure because of emotion, uncertainty, miscalculation, misperception, or the posture of forces to strike first to avoid the worse consequence of incurring a first strike" (Kent and Thaler, 1989: xviii). Therefore, the uncertainty and probability of miscalculation that comes with the introduction of AI to nuclear systems would likely increase crisis instability between states.

HISTORICAL CASE STUDIES

Three specific historical cases can help predict the effects of the onset of AI in nuclear weapons systems. These cases reflect the introduction of new technologies and strategies that risked nuclear escalation but in which great power states managed to prevent conflict. The lessons learned from each case will be useful in formulating predictions, but it is important to note that AI will bring extreme uncertainty that previous changes in nuclear deterrence have not.

First, the Soviet acquisition of ICBMs during the Cold War and the ensuing American "window of vulnerability" mirror the possible advent of AI in nuclear weapons systems. According to Cold War deterrence scholars Richard Lebow and Janice Stein, "By the end of the 1960s, the Soviet Strategic Rocket Forces had deployed enough ICBMs to destroy about half of the population and industry of the United States. It had achieved the capability that McNamara considered essential for MAD [mutually assured destruction]. Sometime in the 1970s the Soviet Union achieved rough strategic parity" (Lebow and Stein, 1995: 173).

In response, the United States pursued a path to build up their stockpile of ICBMs and embark in counterforce doctrine (Johnson, 1983). This period marked uncertainty for the United States, just as the implementation of AI will do for any adversary. However, the Soviet advantage did *not* drive the United States to attack the Soviet Union or develop a new technology that would counteract the ICBMs, which would be in line with the hypothesis of this study. Instead, the United States embarked on a new strategy and aimed to reinstate a balance of power. Nonetheless, AI will introduce a level of uncertainty that ICBMs did not, meaning the two technologies may not create similar environments following their introduction to a state's nuclear weapons complex.

Secondly, President Reagan's counterforce strategies along with the American advantage in surveillance techniques during the Cold War provide another case study to help predict the effects of AI on deterrence. Counterforce strategies offer a unique asymmetry between adversaries, as "one effect of counterforce strategies… is that they provide a rational motive for waging a conventional war even when one expects to lose" (Wagner, 1991: 748). At the same time, according to Austin Long and Brendan Rittenhouse Green (2014), the United States had a significant advantage over the Soviet Union in the realm of intelligence and surveillance regarding nuclear weapons. This came in the forms of ocean surveillance technology for submarines, SIGINT, and Rapidly Deployable Surveillance System units. Altogether, these American advantages along with U.S. counterforce strategy demonstrate a path that adversaries may pursue in order to maximize the costs of waging war against them.

As Wagner (1991) described, counterforce is useful even when a state is losing, so it is a useful deterrent against an adversary. This case represents how adversaries may react if another acquires AI capabilities. Rather than purely pursuing the same route as an adversary, another may alter their strategy or develop a technology that helps counter others.

Finally, veering away from nuclear deterrence, the American and Chinese acquisition of space capabilities surrounding the turn of the century offers another comparison to the future mutual acquisition of AI capabilities. Following China's milestone as it became the third country to launch a person into space in 2003, the United States had a clear choice to make: "America could reach out to cooperate, proposing joint space exploration projects, or it could restrict collaboration and perhaps even decide to pursue a space race akin to the 1960s competition against the Soviet Union" (Moskowitz, 2011).

Out of fear, the United States resisted cooperation. It believed that collaboration would provide a greater technological benefit to China and would create a large risk for the United States. However, Clara Moskowitz (2011) recommends that the United States should view space as only one aspect in the overall U.S.-China relationship. Instead of comparing advantages solely in the context of space, Americans should see collaboration as a way to strengthen ties, increase cooperation in other fields, and maintain stability between the two countries.

Similar to the previous case studies, the Chinese acquisition of space capabilities did not lead to acts of aggression. Altogether, the three cases do not point to the likelihood of AI leading to a breaking point in crisis stability between the United States and China or the United States and Russia. However, as the rest of this study will conclude, AI will introduce more technological and strategic uncertainty than past technologies.

When the Soviet Union developed ICBMs or the Chinese put a person in space, the United States understood the technology, but an ICBM or another feat that the United States had previously accomplished is significantly easier to evaluate than AI capabilities. Rather, AI may appear in a variety of realms as it is not a technology within itself, like Horowitz and Kania remind us. AI is an enabler that will introduce indefinite amounts of uncertainty between adversaries and become far more dangerous to crisis stability than the technologies presented in these case studies.

OPERATIONALIZATION

In order to predict the impact of asymmetric acquisition of AI capabilities through a systematic method, this paper will utilize a series of tables that register possible advantages within the varying uses of AI in nuclear systems for different states. Rather than simply recognizing that there may be qualitative variances regarding how states implement AI, this method illustrates the degree to which different capabilities will impact crisis stability. Although there are a variety of techniques for which a state may incorporate AI into its numerous nuclear systems, this system of operationalization will focus on five primary, general, and likely uses of AI: (1) unmanned nuclear delivery systems, (2) nuclear early warning systems, (3) command and control, (4) data processing, and (5) nuclear weapons countermeasures. This is not to say that there are no other possible applications of AI for nuclear systems, simply that these capabilities provide areas in which major-power states may acquire distinct advantages. The methodology will utilize the five categories as examples for how acquisition of varying proficiencies produces asymmetry and ultimately harms nuclear crisis stability.

In order to compare capabilities between two states, it is beneficial to focus on a state's advantage through AI-enhancement and its reliance upon AI for each category. Simply prioritizing the possession of an AI-enhanced capability neglects the asymmetry that may arise from variances in how states utilize AI-systems. For example, if a state utilizes AI to assist its early warning systems while another relies on AI in its early warning systems to make final decisions (without a human in the loop), the latter has a much stronger reliance upon AI. Similarly, if both states possess AI-enhanced nuclear weapons countermeasures, one may possess an extremely reliable system while the other's system may be faulty or incomplete. In this case, one state has a distinctive advantage over the other regarding countermeasures. Therefore, some consideration of reliance and consequent advantage provides a better reference for measuring asymmetry than pure possession of the technology.

When addressing the total degree of asymmetry that varying capabilities produce, it is important to note that some capabilities have greater weight than others. For instance, the utilization of AI-enhanced unmanned delivery vehicles may worry an adversary more than the possession of AI-enhanced data processing systems. Consequently, when measuring asymmetry, or perceived asymmetry, it is useful to weigh delivery vehicles as providing greater advantage than data processing abilities.

In order to combine these factors, the presence of advantages and their respective weights, Table 1, below, presents a method of predicting asymmetry between states. In this table, the advantages of both states regarding varying capabilities are registered for each category, with "1" representing an advantage while "0" represents the lack thereof. If both states record a "0," then neither state holds a distinct advantage over the other in the respective category. The numbers recorded as "weights of capability" represent the impact that the presence of an advantage in the specific category will have on the total asymmetry in the overall relationship. Finally, if there is a presence of an advantage, that category will produce a score of asymmetry equal to its assigned weight. The overall table output will be the sum of each capability's recorded score of asymmetry.

As opposed to presenting an argument for which state will possess future advantage in each category and how each category should be weighted exactly, this study merely proposes predictions for the purpose of demonstrating the likely increases in asymmetry. These guesses show how acquisitions of varying capabilities may populate this table following how states incorporate AI into their nuclear weapons systems. In this sense, Tables 2-3, below, demonstrate a methodology or tool for predicting asymmetry. Using placeholder values for how the United States, China, and Russia will acquire AI, the tables indicate possible asymmetry that may arise between these major-power states.

The hypothetical relationship between the United States and Russia (in Table 3) scored a 7 while that of the United States and China (in Table 2) scored an 8. When compared next to each other, these values do not have any significance because neither the category advantages nor the weights are tied to a consistent interval level of measurement. The fact that China's score is higher than Russia's does not mean that there is more asymmetry in that relationship.

Rather, these values have significance when compared to other values from the same tables when the inputs change. That is, longitudinal changes (over time) in table output are more meaningful than cross-dyad differences in any single year. The various possible inputs (advantages in capabilities along with the weights) in a specific table dictate the overall table output.

When the U.S.-China analysis produces a score of 8, the policy takeaway should focus on methods to reduce the table output over time, which could occur from the removal of or the emergence of new advantages. A scenario that produces higher table outputs for the same dyad indicates higher levels of asymmetry. The desire to decrease asymmetry would entail efforts to minimize the table outputs so that they approach zero in every category of capability.

Consequences

As this method of predicting asymmetry between the selected major-power states demonstrates, qualitative variance in acquiring AI-enhanced nuclear weapons will increase asymmetry within these relationships. This asymmetry will undoubtedly increase the uncertainty of these states when analyzing the capabilities of an adversary due to the fact that AI is a format of technology, a kind of utility that contains a wide array of unknown variables. A state may be uncertain of how an adversary's AI systems function, the degree to which they rely on AI in these systems, the decision-making autonomy given to the system, etc.

Referring to Kent and Thaler's definition of nuclear crisis stability, that "crisis instability is the condition that exists when either leader feels pressure because of emotion, uncertainty, miscalculation, misperception, or the posture of forces to *strike first* to avoid the worse consequence of incurring a first strike," this increase of uncertainty from AI asymmetry will negatively affect nuclear crisis stability. It follows that as asymmetry increases (or the table outputs presented increase,) the degree of uncertainty will increase, and nuclear crisis stability will continuously decrease.

Counterarguments

After reviewing the case studies presented in this study, it may not seem as if asymmetry truly effects crisis stability to the point that an actor will utilize a preemptive strike. In the historical cases of Soviet acquisition of ICBM's, the American employment of counterforce strategies, and the Chinese rise in space power, no state chose to strike its adversary. These results would lead to the conclusion that asymmetric acquisition of capabilities does not significantly diminish nuclear crisis stability. Since the dawn of the nuclear age, great powers have always found a way to avoid worst case scenarios that might be brought about from rapid technological change.

However, AI provides more uncertainty regarding intention and capabilities than the technologies presented in the old case studies. For example, when the Soviet Union acquired ICBMs, the United States recognized what this meant for their security posture. It was clear what advantage this weapon system provided the Soviets, so the level of uncertainty was relatively low.

In the case of AI, as previously mentioned, states will struggle to determine how states will be able to utilize autonomous systems. Intentions, capabilities, and reliance will all be indeterminate without transparency from great power states that acquire AI. For this reason, AI introduces a new level of uncertainty regarding capabilities that is unprecedented and may have unique effects on nuclear crisis stability. More specifically, the uncertainty surrounding AI-enhanced systems will decrease nuclear crisis stability in a way that previously existing technologies have not.

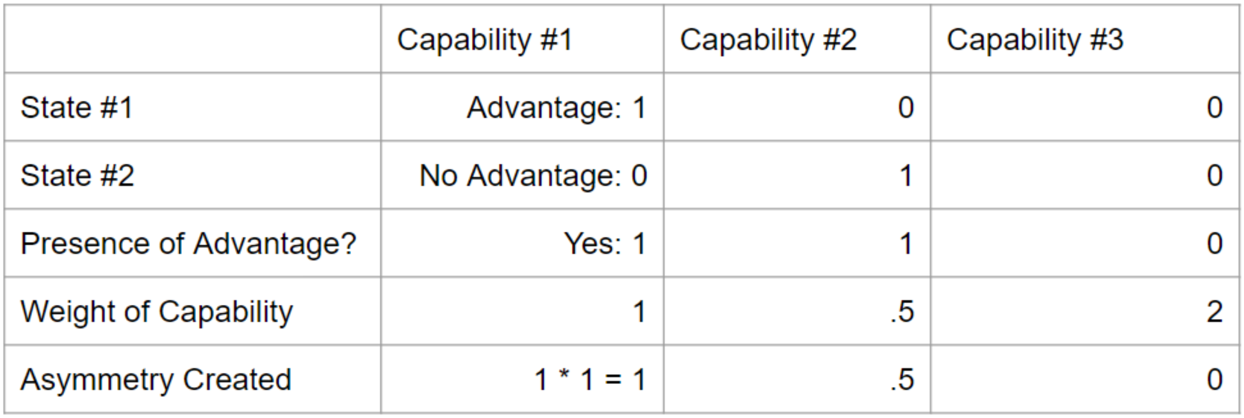
CONCLUSION AND SUGGESTIONS

To reiterate, the method presented in this study demonstrates how crisis stability will decrease as great-power states asymmetrically acquire AI-enhanced technologies and incorporate them—in qualitatively different ways—into their nuclear weapons systems. For policy, this introduces the desire to limit asymmetry between major-power states.

In order for the United States to achieve this goal and preserve nuclear crisis stability, it could pursue three distinct actions. First, it might enhance its intelligence gathering methods that allow it to better understand adversaries' intentions and capabilities regarding AI-enhanced systems. By doing so, the United States will increase its ability to accurately predict AI paths of its adversaries. The United States should then aim to limit asymmetry between itself and adversaries by increasing its own capabilities in the same areas as adversaries. Using strengthened intelligence from the first step would allow the United States to know which capabilities its adversaries are developing, and increase its ability to counter, to stay on par with those adversaries.

Finally, and most importantly, the United States and the international community could work to place controls and regulations on the incorporation of AI in nuclear weapons systems in a bid to maintain transparency. This final step would decrease the number of areas in which states could develop AI-systems and therefore reduce the chances that a state might achieve an advantage over the United States. Altogether, these prudent steps would limit asymmetry between major-power states, prevent uncertainty regarding adversarial AI-enhanced nuclear systems, and ultimately help maintain nuclear crisis stability.

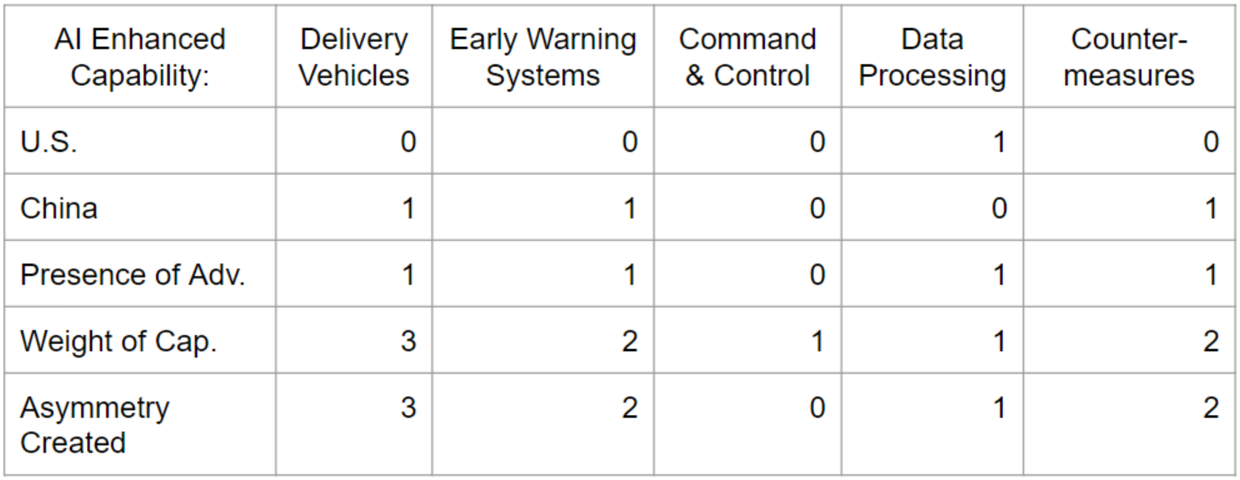
Table 1: Example



	Capability #1	Capability #2	Capability #3
State #1	Advantage: 1	0	0
State #2	No Advantage: 0	1	0
Presence of Advantage?	Yes: 1	1	0
Weight of Capability	1	.5	2
Asymmetry Created	1 * 1 = 1	.5	0

Table Output (Sum of Asymmetry Created): 1.5

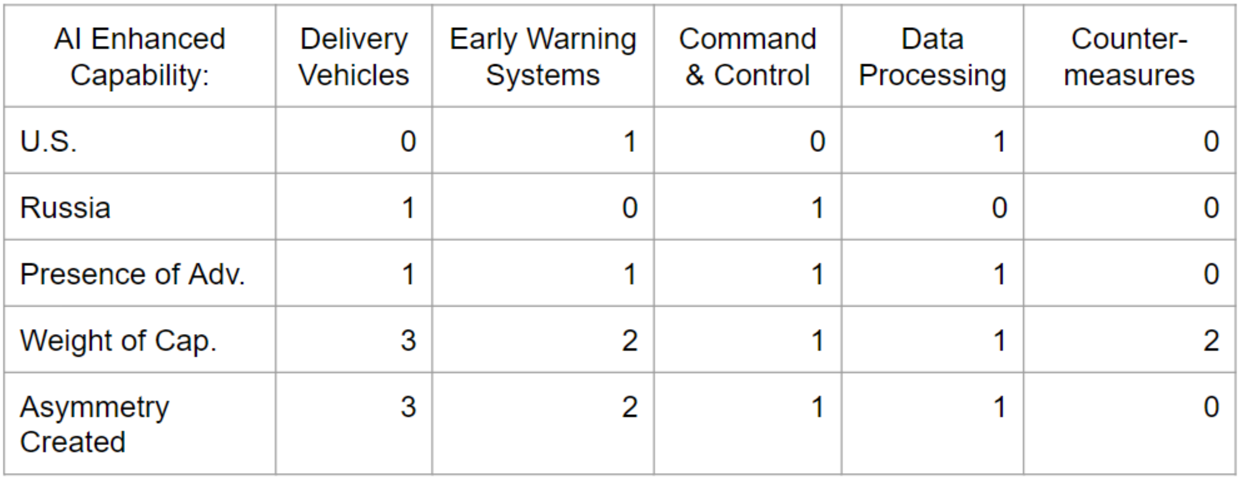
Table 2: U.S.-China



AI Enhanced Capability:	Delivery Vehicles	Early Warning Systems	Command & Control	Data Processing	Counter-measures
U.S.	0	0	0	1	0
China	1	1	0	0	1
Presence of Adv.	1	1	0	1	1
Weight of Cap.	3	2	1	1	2
Asymmetry Created	3	2	0	1	2

Table Output: 8

Table 3: U.S.-Russia



AI Enhanced Capability:	Delivery Vehicles	Early Warning Systems	Command & Control	Data Processing	Counter-measures
U.S.	0	1	0	1	0
Russia	1	0	1	0	0
Presence of Adv.	1	1	1	1	0
Weight of Cap.	3	2	1	1	2
Asymmetry Created	3	2	1	1	0

Table Output: 7

BIBLIOGRAPHY

Cimbala, Stephen. “Chasing Its Tail: Nuclear Deterrence in the Information Age.” *Strategic Studies Quarterly* 6, no. 2 (Summer 2012): 18-34.

Horowitz, Michael C. “Artificial Intelligence, International Competition, and the Balance of Power.” *The Scholar* 1, no. 3 (May 2018): 36–57. https://doi.org/10.15781/T2639KP49.

Jervis, Robert. “Arms Control, Stability, and Causes of War.” *Political Science Quarterly*, vol. 108, no. 2, 1993, pp. 239–253., doi:10.2307/2152010.

Johnson, James. “Artificial Intelligence & Future Warfare: Implications for International Security.” *Defense & Security Analysis* 35, no. 2 (April 2019): 147–169. https://doi.org/10.1080/14751798.2019.1600800

Johnson, Robert H. “Reconsiderations: Periods of Peril: The Window of Vulnerability and Other Myths.” *Foreign Affairs*, Foreign Affairs Magazine (Spring 1983), https://www.foreignaffairs.com/articles/united-states/1983-03-01/reconsiderations-periods-peril-window-vulnerability-and-other.

Kania, Elsa B. “The Pursuit of AI Is More Than an Arms Race.” *Defense One*. Government Media Executive Group LLC., April 19, 2018. https://www.defenseone.com/ideas/2018/04/pursuit-ai-more-arms-race/147579/.

Kent, Glenn A., and David E. Thaler. “First-Strike Stability: A Methodology for Evaluating Strategic Forces.” *RAND Corporation*, 1 Jan. 1989, https://www.rand.org/pubs/reports/R3765.html.

Kissinger, Henry A. “How the Enlightenment Ends.” *The Atlantic*. Atlantic Media Company, August 30, 2019. https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/.

Lebow, Richard Ned, and Janice Gross Stein. “Deterrence and the Cold War.” *Political Science Quarterly*, vol. 110, no. 2, 1995, pp. 157–181., doi:10.2307/2152358.

Long, Austin, and Brendan Rittenhouse Green. “Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy.” *Journal of Strategic Studies*, vol. 38, no. 1-2, 2014, pp. 38–73., doi:10.1080/01402390.2014.958150.

Moskowitz, Clara. “US & China: Space Race or Cosmic Cooperation?” *Space.com*, 27 Sept. 2011, https://www.space.com/13100-china-space-program-nasa-space-race.html.

O'Hanlon, Michael E. “The Role of AI in Future Warfare.” *Brookings*. Brookings, November 28, 2018. https://www.brookings.edu/research/ai-and-future-warfare/.

Pecotic, Adrian. “Whoever Predicts the Future Will Win the AI Arms Race.” *Foreign Policy*, March 5, 2019. https://foreignpolicy.com/2019/03/05/whoever-predicts-the-future-correctly-will-win-the-ai-arms-race-russia-china-united-states-artificial-intelligence-defense/.

Schelling, Thomas C. “The Reciprocal Fear of a Surprise Attack.” *RAND Corporation*, 16 Apr. 1958, https://www.rand.org/content/dam/rand/pubs/papers/2007/P1342.pdf.

Wagner, R. Harrison. “Nuclear Deterrence, Counterforce Strategies, and the Incentive to Strike First.” *American Political Science Review*, vol. 85, no. 3, 1991, pp. 727–749., doi:10.2307/1963848

Cadet Voice
Extended Deterrence and Resilience in the Baltic States

Liam J. Connolly

The following USAFA cadet independent study was supported by the Academy's Nuclear Weapons & Strategy minor and the Cadet Summer Language Immersion Program to Lithuania. With minor formatting changes, the paper here appears as submitted to the USSTRATCOM Larry D. Welch Writing Award and the summer Deterrence Symposium (Omaha, NE), July 31-Aug. 1, 2019, where it won junior division, first place.

Since the end of the Second World War the United States has practiced extended deterrence as a means of resisting Russian expansion and aggression.[1] In Europe, the US has done this with the support of the North Atlantic Treaty Organization. After the fall of the Soviet Union and the end of the Cold War, NATO shifted its focus away from Russia and grew to include several states which had once been part of the USSR; Latvia, Lithuania, and Estonia. However, it was not until after conflict broke out in Ukraine in 2014, and Russia re-emerged as a threat that the alliance was forced to seriously consider defending the Baltics.

For several years, NATO has concentrated its efforts almost exclusively on the structure and placement of military forces with hopes of re-building its once-strong deterrence posture in Europe. The modern, non-kinetic threat to the Baltic Three, however, demands more nuanced solutions which transcend the military sphere. For this reason, the United States and its NATO allies must focus more of their efforts in Northeastern Europe on resilience rather than traditional deterrence. A strategy of resilience in the Baltics must include efforts to counter propaganda and information warfare, build societal cohesion and assimilate Russian-speaking people, and reinforce cyber security in both the private and public sectors. Altogether, these lines of effort will deny the Kremlin the ability to achieve political and strategic goals in the Baltics.

EXTENDED DETERRENCE VERSUS RESILIENCE

Extended deterrence is the concept in which one state guarantees that it will use its military forces not only for its own defense, but also for the defense of its allies. This is done with the intent to persuade a third-party mutual adversary to maintain the status quo in a conflict.[2] Regardless of the domain, deterrence, at its core, consists of two elements: capabilities and credibility. Deterrence is only functional when these elements come together and capabilities are matched with an actual willingness to employ such capabilities.

Signaling "will" is critical when it comes to proving the resolve and legitimacy of an alliance which includes an extended deterrence agreement.[3] The United States has

[1] Second Lieutenant Liam Connolly (USAFA '19) is completing his pilot training.

[2] Schuyler Foerster, ed., *American Defense Policy*, 6th edition. (Baltimore: The Johns Hopkins University Press, 1990).

[3] Matthew Fuhrmann and Todd Sechser, "Signaling Alliance Commitments: Hand-Tying and Sunk Costs in Extended Nuclear Deterrence," *American Journal of Political Science* 58, no. 4 (October 2014): 919–935.

long struggled with figuring out how exactly to signal to adversaries its true willingness to employ military forces and risk personal harm, or even survival, for the sake of another state's security. Signals which are too strong run the risk of escalating the conflict to a point which is too costly for either side.

This was the case in October 1969 when President Richard Nixon ordered the "Madman Nuclear Alert" and heightened the readiness of US strategic forces in hopes of bringing the Soviets to the negotiating table in Vietnam.[4] Soviet leadership, however, was unsure how to interpret the message and experts conclude that the alert represented a serious miscalculation on behalf of US leadership and was ultimately detrimental to stability.[5]

On the other hand, weaker signals may embolden the adversary. In his landmark work, *Arms and Influence*, political scientist Thomas Schelling explained the dangers associated with allowing an adversary to slowly push the limits of a security commitment with tactics that meet, but do not cross, the threshold for retaliation. Schelling coined the term "salami tactics" to describe such activities and argued that, over time, the threshold for retaliation will be forced to rise and the adversary will earn greater freedom to exercise its will.[6]

In the nuclear domain, extended deterrence works to prevent nuclear-capable adversaries from striking allies and partners who lack such capabilities. Nuclear deterrence is closely linked with punishment, or the threat of using strategic weapons to eliminate significant portions of an adversary's civilian population and infrastructure.[7]

Extended nuclear deterrence also works as a means of preventing the proliferation of nuclear weapons. States have no need to pursue their own nuclear program if they feel assured by an ally's capabilities. For decades, the United States' nuclear umbrella has applied to each of its NATO allies and has expanded as the alliance has stretched eastward towards Russia. NATO's 2010 Strategic Concept explicitly states that, "[t]he supreme guarantee of the security of the Allies is provided by the strategic nuclear forces of the Alliance, particularly those of the United States."[8] Simply put, the United States' nuclear capabilities stand as the bedrock of NATO members' national security.

Much like nuclear capabilities, conventional forces also play an essential role in efforts to deter an adversary. Conventional deterrence, however, tends to be more closely associated with denial, or simply, "convincing an opponent that he will not attain his goals on the battlefield."[9] Today, NATO members contribute troops and resources to conventional land, air, and sea forces, some of which are forward staged on the alliance's eastern flank.[10] Given NATO's strictly defensive posture, these forces and their capabilities are meant to influence Russian

[4] Scott Sagan and Jeremi Suri, "The Madman Nuclear Alert," *The MIT Press* 27, no. 4 (Spring 2003): 150–183.

[5] Ibid.

[6] Thomas C. Schelling, "The Art of Commitment," in *Arms and Influence* (New haven: Yale University Press, 1966).

[7] John J. Mearsheimer, *Conventional Deterrence*, Cornell Studies in Security Affairs (Ithaca: Cornell University Press, 1983).

[8] NATO, "Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization" (NATO Public Diplomacy Division, November 20, 2010).

[9] John J. Mearsheimer, *Conventional Deterrence*.

[10] David A. Shlapak and Michael Johnson, *Reinforcing Deterrence on NATO's Eastern Flank* (RAND Corporation, 2016).

leaders' calculus should they consider hostile military intervention within the borders of the alliance.

In the 21st Century, extended deterrence is not strictly limited to the conventional and nuclear domains. A truly effective modern deterrence posture incorporates the full spectrum of warfighting domains to make clear to the adversary that any act of aggression would prove to be too costly in the long term. US Air Force General John E. Hyten, the current Commander of USSTRATCOM, underscored the reality of this dynamic when he said the following:

> The components of our nuclear triad have always been and will continue to be the backbone of our nation's deterrent force. That is where deterrence starts. But today it's more than just nuclear. It requires the integration of all our capabilities…[11]

Deterrence theory was largely born out of the Cold War's bi-polar balance of power which rested on the strength of conventional and nuclear forces, but the dissolution of the Soviet Union has forced a dramatic shift in the global security environment. Adversaries have rapidly worked to gain an asymmetric edge given the United States' and its allies' sizeable conventional advantage.[12]

In turn, warfighting domains which exist beyond the conventional and nuclear spheres have become increasingly relevant in recent years. Most notably, states and non-state actors alike have begun working to exploit the harmful, even militant potential of space and cyberspace. Beyond that, some countries, namely Russia, have incorporated "soft", traditionally non-military tools into military doctrine for achieving political and strategic goals.[13] Rather than existing in separate spheres, economic, diplomatic, and informational tactics are now central to modern warfare. This full spectrum approach to conflict poses a challenge to traditional deterrence theory as leaders today are forced to consider how to address threats and acts of aggression which do not meet the threshold for a violent, military response.

Relative to extended deterrence and traditional methods of maintaining the status quo, resilience offers a more nuanced approach to meeting these modern security challenges. As explained by Dr. Guillaume Lasconjarias of the NATO Defense College, deterrence focuses primarily on the military sphere, whereas a strategy of resilience takes a "whole-of-society approach" to reducing a nation's vulnerability to 21st Century threats such as information warfare and cyber-attacks.[14]

Rather than preventing attacks before they take place, resilience ensures that the acts of aggression are unable to achieve the effects desired by the adversary. As members of the transatlantic political community, NATO member states pride themselves on fostering free and open societies. Unfortunately, this makes the world's most robust military

[11] General John E. Hyten, "2017 Deterrence Symposium Opening Remarks" (Omaha, Nebraska, July 26, 2017).

[12] Herbert Lin and Jackie Kerr, "On Cyber-Enabled Information/Influence Warfare and Manipulation," *SSRN* (August 13, 2017).

[13] Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," *In Moscow's Shadows*, February 27, 2013.

[14] Guillaume Lasconjarias, *Deterrence through Resilience: NATO, the Nations and the Challenges of Being Prepared*, Eisenhower Papers (Rome: Research Division - NATO Defense College, May 2017).

alliance exceptionally weak with regards to these threats.[15]

In practice, resilience includes a wide array of potential endeavors, which range from improving education, building societal cohesion, and strengthening law enforcement among other things.[16] Because the focus is internal, each state's approach to resilience is likely to be unique. However, regardless of the means taken to achieve it, the ultimate goal is to enhance a nation's capacity to withstand prolonged pressure and aggression. To be clear, resilience is not a complete alternative to deterrence but rather a means of reinforcing and supplementing deterrence. Given the challenges and threats currently facing NATO in the Baltics, it is worthwhile to consider a shift in focus from deterrence to resilience in this specific corner of the alliance.

THE THREAT TO THE BALTIC THREE

In 2004 Latvia, Lithuania, and Estonia were welcomed into NATO as full members, and thus became beneficiaries of the alliance's collective defense agreement.[17] Likewise, the former Soviet republics also took their place under the shield of the US nuclear umbrella.
The Baltic States represent the eastern-most edge of the alliance and the farthest that NATO has reached into the Russian sphere of influence.

The Baltics' relationship with Russia dates back to the 18th century and the times when the Russian Empire ruled what is now modern-day Latvia, Lithuania, and Estonia.[18] The Russian Revolution granted the Baltics a brief period of independence, but Soviet occupation took hold in 1940 as Europe nosedived towards the Second World War.[19] Across the Soviet era, the Baltic States stood as part of the geographic "buffer" between Russia and the West.

Following WWII, the communist regime in Moscow implemented so-called Russification policies across the USSR in hopes of, "sovietizing the non-Russian population."[20] Ethnic Russians proliferated throughout the Soviet republics and along with them came Russian language and culture.[21] As a result, over the course of fifty years of Soviet occupation the ethnic composition of the Baltic States was dramatically altered.

Today, in Lithuania, 5.8% of the overall population is ethnically Russian while 8% speak Russian as their primary language.[22] In comparison, 24.8% of Estonians are ethnically Russian and 29.6% speak Russian as their primary language.[23] In Latvia, the state most severely impacted by Russification in the Baltics, 25.6% of the population is ethnically Russian while 33% of citizens identify Russian as their primary language.[24]

In 2014 the Putin regime asserted that Russia has an obligation to "protect" ethnic Russians

[15] Franklin Kramer, Hans Binnendijk, and Dan Hamilton, "Defend the Arteries of Society," *US New & World Report*, June 9, 2015, sec. World Report.
[16] Ibid.
[17] Brad Roberts, *The Case for US Nuclear Weapons in the 21st Century* (Stanford, California: Stanford University Press, 2016).
[18] Romuald J. Misiunas and James H. Bater, "Baltic States - Independence and the 20th Century," *Encyclopedia Britannica*.
[19] Ibid.
[20] Robert J. Kaiser, *The Geography of Nationalism in Russia and the USSR*, Princteon Legacy Library (Princeton University Press, 1994).
[21] Ibid.
[22] "The World Factbook: Lithuania," *Central Intelligence Agency*.
[23] "The World Factbook: Estonia," *Central Intelligence Agency*.
[24] "The World Factbook: Latvia," *Central Intelligence Agency*.

and Russian-speaking people everywhere.[25] Russia, in turn, relied on this claim to justify the annexation of the Crimean Peninsula as well as their support for the bloody separatist movement in Eastern Ukraine.[26] Coupled with the history of the Baltics' relationship with Russia, this policy strongly implies that Latvia, Lithuania, and Estonia are logical targets of Russian belligerence.

Already, the Baltic States have found themselves victims of low-level, non-violent Russian aggression.[27] In 2007, cyber infrastructure in Estonia was struck with massive "distributed denial of service" (DDOS) attacks after the Estonian government decided to move a Soviet war memorial outside the center of the country's capital city, Tallinn.[28] Although there has been no definitive proof that the attacks were ordered or carried out about by the Russian government, Estonian investigators claim to have traced the attacks back to internet users in Russia.

Likewise, Lithuania claims that between 2015 and 2016 the Kremlin was responsible for a wave of cyber-attacks against government systems.[29] More recently, in August of 2017 the Kurzeme region of Latvia experienced a widespread cell-service outage. A Russian ship equipped with electronic warfare capabilities was coincidentally located off Latvia's coast at the time of the outage, and the country's intelligence services strongly suspected a connection.[30] These alleged attacks are consistent with what many officials in the Baltic countries say has been taking place consistently in the region for decades now since the Soviet Union disintegrated.[31]

Russia is also guilty of relying on state-backed media platforms and non-governmental organizations to deliver skewed news and information to Russian speaking populations in the Baltic States.[32] The Russian government's "Compatriots Policy" functions as an arm of the state propaganda machine by linking pro-Russia organizations in the Baltics with necessary funding and resources.[33]

Furthermore, Russian media outlets in the Baltics have become known for expressing anti-Western messages and tend to draw viewers in with higher production quality relative to local media outlets, which communicate in languages other than Russian.[34] Estonia's 2013 Internal Security Service Annual Report asserts that Russian influence operations in the country focus primarily on claims that, "Estonia supports Nazism; Russian-speaking people are discriminated against in Estonia *en masse*; [and] Estonia is a dead-end state that only causes problems for its Western partners."[35] Latvia and Lithuania have also been targets of

[25] "Transcript: Putin Says Russia Will Protect the Rights of Russians Abroad," *The Washington Post*, March 18, 2014, sec. World.
[26] Ibid.
[27] Andrew Radin, "Hybrid Warfare in the Baltics: Threats and Potential Responses" (RAND Corportation, 2017).
[28] Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, vol. 4, no. 3 (Fall 2010): 102-135.
[29] Andrius Sytas, "Russian Hacking Threatens Lithuania's Banks: Survey," *Reuters*, June 6, 2017.
[30] Reid Standish, "Russia's Neighbors Respond to Putin's 'Hybrid War,'" *Foreign Policy*, October 12, 2017.
[31] Andrew Radin, "Hybrid Warfare in the Baltics: Threats and Potential Responses."
[32] Ibid.
[33] Mike Winnerstig, *Tools of Destabilization: Russian Soft Power and Non-Military Influence in the Baltic States* (Swedish Defense Research Agency, 2014).
[34] Andrew Radin, "Hybrid Warfare in the Baltics: Threats and Potential Responses."
[35] *Estonia Internal Security Service Annual Review 2017*, Annual Reviews (Tallinn: Kaitsepolitseiamet, 2017).

claims that the government enforces “fascist” policies.[36]

These examples represent elements of a larger influence campaign adapted to the 21st century information environment and geared towards fracturing ethnic populations in the Baltics while also cultivating general dissatisfaction with the state.

To be clear, these instances alone do not offer concrete proof of an impending Russian offensive with real, kinetic effects. Because Russian aggression in the Baltics thus far has been non-violent and mostly non-attributable, it is evident that they remain wary of the potentially staggering consequences associated with a conventional war between themselves and NATO for the sake of three states whose people have already soundly rejected Kremlin rule twice in the past century. Somewhere there exists a threshold at which point Russia’s provocative actions will be met with retaliation. To operate beneath this threshold and to continue to apply non-kinetic tools with the hope of reigning Latvia, Lithuania, and Estonia back into its personal sphere of influence is Russia’s goal.

In order to understand this, much can be learned from the words of Russian leaders themselves. Mark Galeotti, a senior research fellow at the Institute of International Affairs Prague, famously published and analyzed a 2013 speech by Russian General Valery Gerasimov.[37] Galeotti coined the term “Gerasimov Doctrine” to refer to the speech which loosely outlined Moscow’s perspective on the rapidly-evolving security environment and the use of non-violent methods to achieve political and strategic goals in the aftermath of the Arab Spring**.**

Initial analysis of the speech focused on the idea that non-kinetic activities such as those seen in the Baltics are a prelude to war. In other words, these activities are the Kremlin’s way of “stirring up the battlefield” before *really* engaging in conflict. In a more recent analysis of the speech, however, Galeotti writes, “[t]he point is this: If the subversion is not the prelude to war, but the war itself, this changes our understanding of the threat…”[38]

Galeotti argues that Russia does not equate the line between non-kinetic and kinetic activities with the line between peace and war. Rather, war exists on a wide spectrum and begins with non-violent, non-kinetic activities, which impact the adversary’s political, economic, and psychological condition. This analysis fits the narrative in the Baltic States quite well.

Regardless of whether or not the conflict becomes violent, Russian non-violent aggression, as it stands today, poses a legitimate threat to stability in the Baltics and represents a serious challenge to the sovereignty of these states. An inadequate response from NATO gives weight to concerns that the alliance is not as resolute as it claims to be, and that the United States is not, in fact, a reliable partner in terms of security. For this reason, it is worthwhile to consider the signals that the United States is sending as well as the implications they have for deterring Russia in the Baltics.

[36] Ibid.

[37] Mark Galeotti, “I’m Sorry for Creating the ‘Gerasimov Doctrine,’” *Foreign Policy*, March 5, 2018.

[38] Ibid.

POLICY DEVELOPMENTS

The annexation of Crimea and the onset of the Russian-backed separatist movement in Eastern Ukraine in the spring of 2014 sent shockwaves across NATO. It had been over two decades since Western leaders had seriously considered the possibility of European states being violently attacked from the East. NATO was forced to re-discover its Cold War-era "playbook" and begin seriously thinking about Russia as an adversary once again.

In June of 2014, just months after the onset of the conflict in Ukraine, US President Barack Obama introduced the European Reassurance Initiative.[39] The President's proposal, later approved by Congress, included $1 billion in support of coalition exercises with NATO allies, the deployment of US military advisors, and the improvement of critical security infrastructure in Europe. Each of these lines of effort put special emphasis on Latvia, Lithuania, Estonia, and Poland given their history with and proximity to Russia.

This policy was a clear and swift response to Russia's decision to threaten peace on the continent. It was also a recognition of the fact that, since becoming bogged down in the Global War on Terror and naïve to the reality of great power competition, NATO's force structure and capabilities in Europe had atrophied.

The 2016 election of President Donald Trump gave many proponents of transatlantic collective defense cause for concern. As a candidate and president-elect, Trump openly called into question the efficacy of NATO and Article V several times.[40] Once in office, however, Trump's tone changed. In 2017, President Obama's original policy was re-named the European Deterrence Initiative and spending grew significantly to $3.4 billion annually.[41]

Beyond that, the Trump administration's National Security Strategy (2017) and Nuclear Posture Review (2018) were exceptionally candid in framing Russia as a legitimate, competitive adversary. Under the sub-heading "Promote American Resilience", the most recent NSS asserts that, "actors such as Russia are using information tools in an attempt to undermine the legitimacy of democracies."[42] This accurately describes not just Russia's efforts to interfere in American elections, but also the Kremlin's hybrid strategy in locations such as the Baltics. Later, the document reads, "Russia seeks to restore its great power status and establish spheres of influence near its borders."[43] This is a direct reference to the annexation of Crimea and Russia's greater expansionary ambitions in the former Soviet Union. These quotes reflect the Trump administration's realist perspective on international affairs and a break from the Obama administration's optimistic outlook on relations with Russia.

With regards to the developments in the broader alliance, NATO heads of state and government gathered in Wales in September of 2014 with hopes of charting a new path forward in the face of a renewed, looming threat.[44] Leaders agreed that the alliance

[39] Office of the Press Secretary, "FACT SHEET: European Reassurance Initiative and Other U.S. Efforts in Support of NATO Allies and Partners," *Whitehouse.gov*.

[40] Jenna Johnson, "Trump on NATO: 'I Said It Was Obsolete. It's No Longer Obsolete.'," *The Washington Post*, April 12, 2017, sec. Post Politics.

[41] Jen Judson, "Funding to Deter Russia Reaches $6.5B in FY19 Defense Budget Request," *Defense News*.

[42] United States, "The National Security Strategy of the United States of America" (President of the United States, December 2017).

[43] Ibid.

[44] NATO Heads of State and Government, "Wales Summit Declaration" (NATO, September 5, 2014).

needed to develop and implement an updated deterrence posture and took steps to begin restoring the foundations of collective defense in Europe. Among these steps was the pledge by each member to spend 2% of GDP on defense, as well as the establishment of the Very High Readiness Joint Task Force (VJTF).[45] The VJTF was to be brigade-sized and capable of responding to dynamic threats across the spectrum of warfighting domains.

NATO leaders gathered once again in Warsaw in 2016 and laid out a series of decisions meant to strengthen deterrence. Chief among these decisions was the introduction of the Enhance Forward Presence. This initiative directed the development and deployment of four multi-national, defensive battalions in Latvia, Lithuania, Estonia, and Poland respectively.[46] In Warsaw, the allies also nominally agreed to enhance resilience. NATO's definition for resilience, however, was narrow in scope and strictly related to response after an *armed* attack.[47]

Altogether, there is no question that the United States and NATO have made notable progress with regards to restoring conventional deterrence in Eastern Europe, specifically in the Baltics. These developments, however, have remained almost entirely tied to the military domain and do little to address the most pressing threats actually facing Latvia, Lithuania, and Estonia. Fighter jets, warships, and tanks ultimately cannot prevent the spread of propaganda or attacks in the cyber realm.

RECOMMENDATIONS

Thinking along the lines of resiliency, NATO must look beyond strictly the military dimension and take a much broader approach to denying Russia its goals in the Baltics. There are a number of key areas in which the United States and allies ought to invest and turn their attention towards.

For example, media outlets associated with the Russian state propaganda machine play a central role in the Kremlin's influence strategy in the Baltics.[48] Unfortunately, many TV channels, radio stations, and digital outlets with pro-European slants do not broadcast or publish their work in Russian. Those who are multi-lingual have access to a wide variety of news sources (English, Latvian/Lithuanian/Estonian, and Russian) and are able to see-through absurd Russian propaganda.[49] However, members of society who, to begin with, are most vulnerable to Russian influence are left to consume media from pro-Kremlin sources, which also tend to have higher production quality, thus solidifying interest from viewers.[50]

Essentially, there exist separate information spheres which are sharply divided by language. Working to ensure that Russian-speaking people in the Baltics have access to free and fair media will make them less susceptible to Kremlin-generated talking points and decrease dissatisfaction with the state.

[45] Guillaume Lasconjarias, *Deterrence through Resilience: NATO, the Nations and the Challenges of Being Prepared*.

[46] NATO, "Warsaw Summit Key Decisions" (NATO Public Diplomacy Division, February 2017).

[47] Ibid.

[48] Mike Winnerstig, *Tools of Destabilization: Russian Soft Power and Non-Military Influence in the Baltic States*.

[49] "Disputing Putin: How the Baltic States Resist Russia," *The Economist*, January 2019.

[50] Mike Winnerstig, *Tools of Destabilization: Russian Soft Power and Non-Military Influence in the Baltic States*.

Radio Free Europe/Radio Liberty, a US government funded endeavor, has done work along these lines since the Cold War and claims to have, "played a significant role in the collapse of communism and the rise of democracies in post-communist Europe."[51] RFE/RL discontinued services directed specifically for the Baltics in 2004.

Along the same lines, ensuring the assimilation and enfranchisement of ethnic Russians and Russian-speaking people in the Baltics is also of great importance. This issue most directly pertains to Latvia, the Baltic state most heavily impacted by Russian immigration during the Soviet era. According to the European Network on Statelessness, roughly 230,000 people currently living in Latvia (about 12% of the total population) fall under the classification of "non-citizen".[52] This is largely the result of harsh laws passed in the early 1990's which prevented those who arrived in Latvia during Soviet times from becoming fully naturalized citizens. Non-citizens in Latvia are denied the opportunity to participate in formal political processes, cannot work in government, and do not have freedom of mobility within the European Union.[53]

To make matters worse, the general use of Russian language in Latvia has also faced legal restrictions. A 2018 law approved by Latvia's parliament and president severely limits the use of Russian language in schools across the country despite the fact that many students speak and understand little to no Latvian.[54]

Both Lithuania and Estonia have taken more progressive approaches to ensuring that Russians living within their borders have opportunities equal to those of their ethnically native neighbors.[55] Yet, in an effort to preserve its sovereignty and erase the legacy of Soviet occupation, Latvia effectively played into the hands of Kremlin-backed propagandists and provoked the birth of pro-Russian political movements within its borders.[56] In order to counter the impact of such movements, NATO allies ought to encourage Latvia to adopt policies similar to those of its neighbors to the north and south, which open the door for citizenship and tolerate the use of Russian language in official capacities.

NATO has recognized the threat of cyber warfare and much progress has already been made with regards to cyber security in the Baltics. For example, upon request from Estonia in 2008 the alliance established the Cooperative Cyber Defence Centre of Excellence. The size and scope of this entity's responsibilities has grown over the course of the past decade, and it remains responsible for research and implementation of technology, operations, strategy, and law relating to the cyber domain.[57] With the assistance of allies, the Baltics' security apparatus to include military, law enforcement, and intelligence entities has become hardened against cyber-attacks.

However, one of the greatest remaining challenges with cyber security in the Baltics is the threat to private, non-governmental

[51] A. Ross Johnson, "History of RFE/RL," *Radio Free Europe/Radio Liberty*.

[52] Jo Venkov, "European Network on Statelessness," *Not Just a Simple Twist of Fate: Statelessness in Lithuania and Latvia*, October 2018.

[53] Ibid.

[54] Lucian Kim, "A New Law In Latvia Aims To Preserve National Language By Limiting Russian In Schools," *National Public Radio*.

[55] Jo Venkov, "European Network on Statelessness."

[56] Andrew Higgins, "Populist Wave Hits Latvia, Lifting Pro-Russia Party in Election," *The New York Times* (New York, October 7, 2018), sec. Europe.

[57] "About Us," *Cooperative Cyber Defence Centre of Excellence*.

entities. Since the end of the Cold War, many elements of national security and defense which were previously the responsibility of the state have been contracted out and turned over to the private sector. This is especially true with regards to transportation and communication networks, both of which are vulnerable to cyber-attacks.[58]

Valuable organizations and networks which are not directly connected to national security or NATO are also subject to threats in the cyber realm. This includes media outlets, internet providers, cell networks, health care facilities, banks, and energy infrastructure among many other things. Latvia, Lithuania, and Estonia each pride themselves on having fostered a unique culture of technological innovation and expansion.[59]

As a result, nearly everything and everyone in this region is, in some way, connected and dependent upon the internet. Evidence shows that Russia clearly understands this dependency and has at least begun to explore methods to exploit weaknesses in the cyber domain in the Baltics' private sector. In recent years, cyber operatives connected to Russia have infiltrated and impacted energy infrastructure, banking systems, and cell service networks in the Baltics.[60]

Loss of access to any of these services could cripple the economy and shake citizens' faith in the state. NATO, backed by the United States influence and resources, must expand the cooperative relationship between the public and private sectors with regards to cyber security. Moving forward, military, intelligence, and law enforcement organizations in the Baltics must work with civilian partners to ensure that the cyber realm is secure.

CONCLUSION

Extended deterrence, as traditionally practiced by NATO, provides an outdated model for security in Latvia, Lithuania, and Estonia. Today, the threat from Russia facing the newest and most vulnerable members of the alliance transcends the military domain and includes a wide array of subversive, non-violent, and non-kinetic activities. Increasing the number of allied forces in the region and improving interoperability demonstrate a strong commitment to deterrence. However, the likelihood of a conventional, kinetic attack is low.

The presence of soldiers and warplanes cannot prevent information warfare or cyber-attacks before they take place. For this reason, NATO must begin strengthening resiliency in the Baltics. By improving the condition of Russian speaking people, combating propaganda, and strengthening cyber security in the private sector, the Baltics will be more capable of enduring Russian aggression over time.

[58] Guillaume Lasconjarias, *Deterrence through Resilience: NATO, the Nations and the Challenges of Being Prepared*.

[59] Alison Coleman, "Why Business Is Booming In the Baltics," *Forbes*, September 20, 2015.

[60] Gederts Gelzis and Robin Emmott, "Russia May Have Tested Cyber Warfare on Latvia, Western Officials Say," *Reuters*, October 5, 2017.

Book Review
Tom Nichols, *The Death of Expertise: The Campaign against Established Knowledge and Why It Matters* (NY: Oxford University Press, 2017), 252 pp.

Damon Coletta

This review is dedicated to Lt Gen (ret.) Brent Scowcroft, twice National Security Advisor and one-time head of the Department of Political Science, U.S. Air Force Academy. If he is looking down on our work today, we hope he liked this book, Death of Expertise*, by a much admired Naval War College professor and enjoyed our department's enthusiasm for participating in the conversation. Thank you, Gen Scowcroft (1925-2020).*

Naval War College professor Tom Nichols built upon his popular essay in the *Atlantic* to deliver a blunt warning.[1] After a venomous election in 2016 that swept the incumbent party from power, American democracy was in for a rough go. Sir Lawrence Freedman (Emeritus, King's College, London) employed the term "polemic" to characterize *Death of Expertise*, and Nichols did take shots at certain celebrities professing bizarre, defiantly unscientific, nostrums for better health. Yet, Nichols, the strategist and foreign policy expert, had a loftier aim and a deeper message in mind than disarming the army of nattering nabobs on American social media.

Expertise is also a eulogy for a young and strong United States in geopolitical terms, for a period, a lifetime ago, when Americans from all walks attentively tuned the radio to absorb learned rhetoric of the Commander-in-Chief and earnestly assume their civic obligations as ordinary citizens in time of world war. Nichols' framing of the problem is at once profoundly conservative and anti-Trump, at least the popular Trumpism in 2016-2017 that pilloried expert professionals from doctors to diplomats, then ran them out on a rail from positions of influence on America's future.

For the long decline of American democracy, Nichols located the mortal wound in the decade of the 1970s. Failed intervention in Southeast Asia and the frustrated civil rights movement at home culminated in violent protest, riots, and proliferation of crimes—kidnappings, assassinations, bombings, and a White House scandal—splashed across national media. America appeared to recover from the discord at first, claiming victory in the Cold War and achieving a long sail of peace and economic growth during the 1990s. Nichols explained, though, how new factors such as emergence of the Internet, customer-oriented concessions in higher education, and fragmentation of the media into cult punditry accelerated internal bleeding, cementing then spreading as a cancer popular skepticism of professional expertise.

If Nichols' diagnosis is correct, the American experiment is in trouble. Nichols' anchoring chapter on "Death of Expertise and Democracy" pointed out that experts across

[1] Damon Coletta is 2020-2021 Scowcroft Professor in the Dept. of Political Science, U.S. Air Force Academy, author of *Courting Science: Securing the Foundation for a Second American Century* (Stanford, 2016), and coeditor of this journal.

the professions are losing patience with the public and, for their part, regular citizens are in no mood to grant credentialed pontificators the benefit of the doubt. With general breakdown of communications between the professions and society, Nichols wrote, "all things are possible," including "the end of democracy," either by foreign intrigue or policy paralysis of republican government. These were the very threats to the American experiment George Washington spotlighted as he bequeathed the presidency in his classic 1796 Farewell Address.

Nichols, though, offers a fresh twist on the *Washington Post*'s latest motto, "Democracy dies in darkness." For Nichols, the looming darkness is not what most Americans would fear at onset, say, sudden suppression by a man on horseback or a popular fascist crushing the minority's capacity to see or seek. Rather, the darkness is insidious. There is too much light at first, too much access, so many choices that free citizens lose their way. Anyone can become informed. Every citizen's judgment counts as good as the next opinion—on health, justice, science, or public policy.

In his telling, Nichols approached the nineteenth century aristocrat Alexis de Tocqeville's *Democracy in America.* Freedom and democracy do not actually suffocate in pitch darkness. They drown in blooming, buzzing confusion—restless citizens chasing every which way an unholy Grail of universal equality. Such rigid uniformity in tackling the world's problems precludes specialization and excellence in the professions, undermines a key principle of social cohesion, and dashes hopes for a great, diverse Union that can be a beacon of human liberty as John Winthrop's City on a Hill.

To this point, Nichols trod on familiar ground, but he also wanted to argue that this time is different. If expertise can die only once, the American people have only one shot. Once they kill philosophy by arresting its seers who profess truths just beyond the ken of ordinary folk, once they tear down talented specialists and lock them away from societal influence, there is no going back to science based policy. Once unmoored from expertise, the free polity cuts its engines, adrift forever.

Here, Nichols may have exaggerated his indictment, with the result that the death of expertise appears a most urgent threat to democracy's survival, but the obligation of experts to do something about it is practically set aside. Sure, educated professionals must remain cognizant of limits of their discipline and graciously accept defeat when politicians or layperson clients decide to reject best advice. Nichols reserved the real task, though, for citizens, who *en masse* must find the wherewithal to look up from their daily cares and restore national faith in scientific elements of liberal education—that this process will produce experts who want to do good *and* know what they are talking about.

The great twentieth century (expert) political scientist Samuel Huntington thought differently, that is, in terms of cycles or what he called creedal passion periods. The American Revolution and struggle to ratify the United States Constitution represented the first such period. Every sixty years or so, a generation would rise to challenge established ways of the democratic Republic, in short, to tear down old expertise and construct new institutions to shoulder the nation closer toward its founding ideals. American democracy, Huntington wrote, was a "disappointment only because it is also a hope." The latter half of the American cycle, the recovery or upswing, is absent from Nichols' account, and this omission changes everything.

The American people are not killing expertise or the possibility of creative specialization in society. In their freedom, they are alert—not confused—when creaking social structures no longer keep pace with demand for prosperity and greater justice under liberal democracy. Once the old towers have fallen, there will come a historic moment, a Bretton Woods convocation or a Sputnik imperative, when expertise attuned to contemporary challenges is called back to life in service to the national experiment. The upshot of Huntington's theory of the case, as opposed to Nichols', is the public will probably follow their usual cycle. It is the *experts* who need to be prepared to act well when their moment arrives.

While both Nichols and Huntington would be cautious about predicting just where democracy is in a political cycle while relations with science are in flux, the 2016 election surprised most experts. Three years later, President Trump was impeached by the House and soon thereafter acquitted by the Senate on contradictory, partisan votes. The tumult in Washington may turn out to be symptomatic, announcing an unusual dearth of trust in expertise or professional staffs that ought to bring warring factions together and set a wise course for the country. The COVID-19 pandemic may have hit too soon in the cycle for expert professionals to slip into place and ferry elected politicians expeditiously through twin health and economic crises.

Experts, nevertheless, are on the case, and there may yet be an opening with the American people to help political leaders, divided across federal branches and individual state governments, in record time implement science based policy tied to COVID vaccines.

Closer to the substantive focus of this journal, year 2019 also saw the inauguration of the U.S. Space Force (USSF), a separate service under the department and civilian secretary of the Air Force. The birth of USSF manifests a stunningly swift shift in political headwinds against its creation a few short years before. Many defense policy experts counseled *against* the move.

Rather than the death of expertise, though, USSF coming into being presents an opportunity, albeit on a different plane from COVID—one of those moments at the upswing of Huntington's passion periods for another epistemic community to apply its specialized knowledge in service to the greater good.

Talented members of the professional classes, meanwhile, have no time to wait for a positive swing in the public mood. They will come around, according to the existing pattern, the cyclical relationship between democracy and the professions. Still, military officers and civilian defense experts have immediate social responsibility to help their political masters, representatives accountable to the people, lead public opinion toward workable solutions for the new Space Force as well as the current pandemic.

Expertise is not dying. Contemporary politicians merely sent its purveyors back to the woodshed to work a bit harder, to sharpen their skills and knowledge for success against novel national challenges. Adapting and applying expertise within a democratic political context will soon be the sacred labor of educated elites on space, health, the environment, education, and the economy.

Nichols' recommendations in his book for today's experts unfortunately languished at second-priority status. The best professionals *already* recall, always remember, that they are the advisers not the deciders, the servants not the masters, of democratic society and republican government.

Today’s experts have multiple jobs to do. Politicians backed by the public are requesting help on a variety of national issues that cut across academic disciplines and tap a mix of professions. These will not always see eye-to-eye on the way forward. Informed voices will not always cohere. Nevertheless, public clamor for genuine expertise is likely to mount, not die away, after the 2020 election. Expert professionals will abandon their duty if they shrink from the kind of politicized popular criticism that so exasperated Nichols. If the current creedal passion period will soon end, as in past cycles, the professional response to enormous national challenges has to be sober recognition of false starts, clear explanations of lessons learned from hard-won experience, and steady, confident management of accountable government in a great democracy.

Notes for Contributors to *Space & Defense*

Space & Defense seeks submissions that will contribute to the intellectual foundation for the integration of space into overall security studies.

Indeed, the emergence of space as a unique and critical element in national security, economic security, homeland security, cyber security, environmental security, and even human security has persuaded us that this line of inquiry is vital to innovation for international security.

Contributions are welcome from academic scholars and policy analysts at think tanks and research institutes; senior management and policy officials from international and governmental agencies and departments relevant to space and security issues; senior management and policy officials from organizations responsible for critical national and international infrastructures that rely upon space; major aerospace corporations; scientists and engineers interested or involved in space and security policy issues; military officers and operators in relevant units, commands, and in staff colleges and service academies.

The journal welcomes submissions of scholarly, independent research articles and viewpoint essays. There is no standard length for articles, but 7,500 to 10,000 words, including notes and references, is a useful target for research articles, and viewpoint essays should be in the range of 2,500 to 5,000 words. The opinions, conclusions, and recommendations expressed or implied within *Space & Defense* are those of the contributors and do not reflect those of the Eisenhower Center for Space and Defense Studies, the Air Force Academy, the Air Force, the Department of Defense, or any other agency of the United States Government.

Articles submitted to *Space & Defense* should be original contributions and not under consideration for any other publication at the same time. If another version of the article is under consideration by another publication, or will be published elsewhere in whatever format, authors should clearly indicate this at the time of submission. When appropriate, all articles are required to have a separate abstract of up to 250 words that describes the main arguments and conclusions of the article.

Details of the author's institutional affiliation, full address, and other contact information should be included in a separate file or cover sheet.

Contributors are required to submit all articles electronically by email attachment as a Microsoft word file (.doc or .docx format).

Contributors should not submit PDF files. All manuscripts submitted to *Space & Defense* need to be double-spaced with margins of 1 inch or 2.5 cm, and all pages, including those containing only diagrams and tables, should be numbered consecutively. It is the author's responsibility to ensure when copyrighted materials are included in a manuscript that the appropriate copyright permission is received by the copyright holder.

Address manuscripts and all correspondence to:
Dr. Damon Coletta, Damon.Coletta@usafa.edu (e-mail),
or 719-333-2270.

On the basis of peer reviews for research articles, the academic editors will make a final decision for publication. If required, the author(s) will be required to make additional changes and corrections as a result of the external peer review.

TABLES AND FIGURES

All maps, diagrams, charts, and graphs should be referred to as figures and consecutively numbered and given appropriate captions. Captions for each figure should be submitted on the same page as the figure to avoid confusion. Tables should be kept to a minimum and contain only essential data. Each figure and table must be given an Arabic numeral, followed by a heading, and be referred to in the text. Figures and tables are not to be embedded in the text. Each table and figure should be clearly labeled. In the text, make sure and clearly explain all aspects of any figures or tables used.

STYLE

Authors are responsible for ensuring that their manuscripts conform to the style of *Space & Defense*. The editors will not undertake retyping of manuscripts before publication. Please follow the Chicago Manual of Style.
Listed below are some additional style and writing guides:

- Dates in the form: 1 January 2009.
- Headings (bold, ALL CAPS, title case and centered).
- Subheadings (bold, italic, title case and centered).
- Acronyms/abbreviations should always be spelled out in full on first use in the text.
- The 24-hour clock is used for time, e.g., 0800, 1300, 1800.
- Use percent rather than % except in figures and tables.
- For numbers, spell out numbers less than 10.
- Make use of 21st style where appropriate.
- Keep capitalization to a minimum.
- Concise paragraphs and sentences are desirable.
- Avoid a paper that is just descriptive; rather engage the literature and provide analytical rigor and assessment.
- Avoid policy recommendations in the analysis part of paper; leave this, if applicable, for a separate section at the end of the paper.
- Define all new terms used in paper.
- Avoid hyphenated words when possible (e.g., low Earth orbit).
- Avoid the use of passive voice when possible.
- Footnotes, numbered consecutively with a raised numeral in the text, use the Insert-Preference-Footnote function of Word.