AUTONOMOUS DEFENSIVE SPACE CONTROL

VIA ON-BOARD ARTIFICIAL NEURAL NETWORKS

Michael T. Manor, Major, USAF
April 2007

Blue Horizons Paper
Center for Strategy and Technology
Air War College

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **APR 2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**
4. TITLE AND SUBTITLE **Sutonomous Defensive Space Control via On-Board Artificial Neural Networks**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,Air War College,Center for Strategy and Technology,Maxwell AFB,AL,36112**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES		
14. ABSTRACT **see report**		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**50**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

DISCLAIMER ii
ILLUSTRATIONS iv
ACKNOWLEDGEMENTS v
ABSTRACT vi
ENSURING FREEDOM OF ACTION IN SPACE 1
CURRENT THREATS AND U.S. SPACE POLICY 5
- Why the U.S. Has Fallen Behind 6
- What Caught the U.S.'s Attention? 7
- The Threat Today 9
- U.S. Space Policy 11

HOW ARTIFICIAL NEURAL NETWORKS WORK 12
- How Neural Networks Learn 13
- Variations in Neural Network Design 14
- Satellite Applications 15
- Challenges 18

POSSIBLE SPACE SUPERIORITY SCENARIOS & THEIR IMPACTS ON NN DESIGN 21
- Humpty Dumpty 22
- Three Little Pigs 23
- Tortoise and the Hare 23
- Chicken Little 24

CONCLUSIONS AND RECOMMENDATIONS 25
- Operational Impact 25
- Recommendations 26

APPENDIX A: METHODOLOGY 29
APPENDIX B: FURTHER RESEARCH 31
APPENDIX C: IMPACT OF COMMERCIAL MARKETS AND NON-STATE ACTORS 33
- Commercial Market Interest 33
- Rise of the Non-State Actor 34

GLOSSARY 36
BIBLIOGRAPHY 37
NOTES 40

Illustrations

	Page
Figure 1 Chinese ASAT Launch	5
Figure 2 Maethner's Space Superiority Scenarios	22

Acknowledgements

I would like to thank my wife, Tracey, and daughters, Brooke and Lindsey, for their unwavering support throughout this and every other journey on which the Air Force has taken us. I would also like to thank my ACSC Blue Horizon instructors and seminar mates for challenging me to think beyond the realm of the present, and to dream the big dreams. Finally, I would like to thank Starbucks Coffee for developing a product that enables so many to accomplish so much.

Abstract

Future advances in neural network technology, coupled with increased computer processor capability, may create an opportunity to develop systems that enable satellites to autonomously differentiate, detect and defend against attacks. The Air Force should take advantage of this potential opportunity by investing the necessary resources for the development of space-based neural networks.

An artificial neural network (ANN) or commonly just neural netwo**rk** (NN) is an artificial intelligence system created to mimic the ways and methods in which our own brains respond to and learn from inputted stimuli.[1] Each of these networks consists of an array of neuron-like gates programmed to take action once a designated threshold is crossed.[2] These ANN are adaptive, and learn through continued processing of inputted stimulus while developing a memory by storing the actions it takes in response to this stimulus.[3] This memory gained through storing data enables ANNs to become somewhat autonomous over time because they have the ability to recall a given action taken based on a given input received.

Computer processing will likely continue to increase in power while decreasing in size.[4] Expanded processing capability could potentially enable the placement of neural networks, requiring significant processing power and storage capacity, on-board satellites that must contend with size and weight limitations. At the same time, advances in the fidelity and sensitivity of neural network capabilities might give spacecraft processing units (spacecraft brain) more "intelligence," or ability to give raw data meaning. The merging of increased processing power with a reliable neural network will potentially give a spacecraft the ability to recognize, through its telemetry, that something is attacking it. Furthermore, the spacecraft might then be able to delineate between possible types of attack (e.g. directed energy, kinetic, co-

orbital), and autonomously respond, defensively, to an attack in a method that could keep it in mission operations.

Ensuring Freedom of Action in Space

In this new century, those who effectively utilize space will enjoy added prosperity and security and will hold a substantial advantage over those who do not. Freedom of action in space is as important to the United States as air power and sea power.

—President George W. Bush
U.S. National Space Policy, 2006

Why Does This Matter?

The United States Department of Defense's (DoD) reliance on space systems for joint military operations is a stark reality today. Operations DESERT STORM, ALLIED FORCE, DELIBERATE FORCE, and ENDURING and IRAQI FREEDOM each used a combination of joint forces and space assets, and provide the backdrop for what has become the new American standard for bringing decision superiority and precise effects to the battlefield. Space systems have helped compress the kill chain[5,6], dramatically improved precision and have given U.S. decision-makers global access and global presence thereby providing options to see, hear, act and know. These recent campaigns make it clear that the DoD prefers to fight with, rather than without, space.[7] This increasing reliance on space systems introduces significant vulnerabilities because the DoD currently lacks a robust capability to protect its space assets.[8,9] Unless the U.S. can continue to ensure freedom of action in space, the asymmetric advantage space systems provide is in jeopardy.

Today the U.S. cannot consistently detect, identify, attribute, and respond to an attack on its space systems.[10] Our systems are vulnerable because they operate in predictable orbits over potentially hostile areas without escort. U.S. satellites essentially fly blind, and others have the capability to track and engage them. In other words, an adversary can find, fix, track and target a

U.S. satellite without the U.S. knowing it is even happening. This is of major concern because the U.S.'s most treasured space assets, its intelligence satellites and manned space flights, operate in Low Earth Orbit (LEO).

Threats to our space systems have grown significantly, as nations continue to not only pursue the means, but also demonstrate the will to deny the United States and its allies the benefits of their space systems. According to press accounts, China used lasers to blind one of these U.S. spy satellites.[11] At one time, this act was unthinkable, but now it is only a footnote in an ever-increasing hostile space environment with many more similar examples. To make matters worse, U.S. dependence on space systems makes these threats significant when looking at the potential impacts of similar attacks during wartime.[12]

To ensure its space assets are available when the U.S. needs them, the U.S. must maintain a level of space superiority. Space superiority is the level of control in space that ensures our space platforms can continue to provide sufficient capabilities and effects for our air, sea, and land forces.[13] Achieving this freedom requires three distinct operational capabilities: space situational awareness, the ability to see and understand what is occurring in space; offensive space control, the ability to deny enemies use of their space systems; and defensive space control, the ability to protect ones space systems from enemy disruption.[14]

An on-board artificial neural network (ANN) is one possible method that could help the U.S. compensate for present vulnerabilities by giving its satellites the required awareness and understanding to protect them during an adversarial attack. In terms of gaining space superiority, ANNs would benefit the U.S. by enhancing its capability to gain better space situational awareness while providing a means for improved defensive space control.

Artificial neural networks are artificial intelligence systems created to mimic the ways and methods our own brains respond to and learn from inputted stimuli.[15] Each of these networks consists of an array of neuron-like gates programmed to take action once a designated threshold is crossed.[16] Like our brains, these systems learn based on the continued processing of inputted stimuli, and develop a memory by storing the actions it takes in response of them.[17] This memory gained, through storing data, enables ANNs to become somewhat autonomous over time because they have the ability to recall a given action taken based on a given input received.

Although an all-knowing satellite with human-like intelligence seems far off, the Air Force is currently using neural networks on a limited basis in similar roles. One such neural network, Satellite as a Sensor (SAS), is a tool that provides anomaly recognition for a variety of Air Force Space Command satellites.[18] SAS has the ability to warn a ground operator when a spacecraft telemetry point is "out of bounds" of what it has learned to be normal for that particular spacecraft. The delineation between what is normal telemetry and what is not is the first step in being able to solve the problems of attack detection and attack identification. In other words, once a neural network understands what the data readings are for normal operations, it can then recognize when something different, possibility an attack, is occurring.

However, this particular neural network is not without limitations. SAS requires significant processing power, data storage capacity and has to complete validation testing during a "live fire" space control event. In addition, SAS is a ground-based system, used specifically on satellites in Geosynchronous Earth Orbits (GEO). This is significant because GEO satellites are always in view of their ground stations, and ground operators have constant access to these satellites' telemetry. If attacked, an operator would most likely see that something was happening to the vehicle instantly because of this constant flow of data, with or without the use

of SAS. In addition, SAS is a supervised neural network requiring significant "learning" time and operator intervention to give meaning to or label events as they occur.[19] All of which limits the ability of this particular neural network to be pushed into an autonomous Defensive Space Control role for LEO satellites that consistently travel out-of-view of ground stations, and would be required to function without the benefit of ground operator intervention.

The DoD should develop artificial neural networks that can ensure the safety of these LEO satellites as well. If SAS truly is the best Defensive Space Control neural network the DoD currently has, it must invest in other options to protect its most vulnerable systems. A more adequate on-board neural network could provide protection for these satellites even when they are out of view of ground stations, and do not have the benefit of ground operator intervention. Essentially, a neural network could put satellites into a protective mode to shield it from directed energy (i.e. jamming or lasing) during the duration of an attack, and feed other like systems for increased overall situational awareness.

Directed energy is only one of the many threats U.S. satellites face. ANNs might not be effective against other types of threats such as a direct assent or co-orbital ASATs. The proposed use of ANNs in this research paper is not to eliminate theses types of threats, but merely to minimize their intended effect as much as possible. Appendix B contains further discussion of this delineation for effective NN use, and the possibility of them sharing situational awareness information with other systems.

The following research further explores the idea of NN use on satellites. The examination of the current threat environment and U.S. space policy will illustrate the need for such protective systems. A technical discussion of NNs, and the feasibility of their use on satellites follows this study of the external and internal environment. In addition, four possible

future scenarios will then describe alternative conditions and their influence on NNs development. Finally, the paper will conclude with recommendations for NN use as well as steps the Air Force can take to further NN advance. Appendix A contains a more detailed discussion of the methodology used within this research paper.

Current Threats and U.S. Space Policy

Know thy enemy and know thy self...

—Sun Tzu
The Art of War

In attempting to understand why the Air Force should use artificial neural networks for protecting satellites, it is important to first understand the contextual factors both outside and inside the USAF. In other words, which external actor threats make these space control programs critical for U.S. development, and which challenges have hindered the Air Force's progress toward developing a robust and comprehensive space control program.

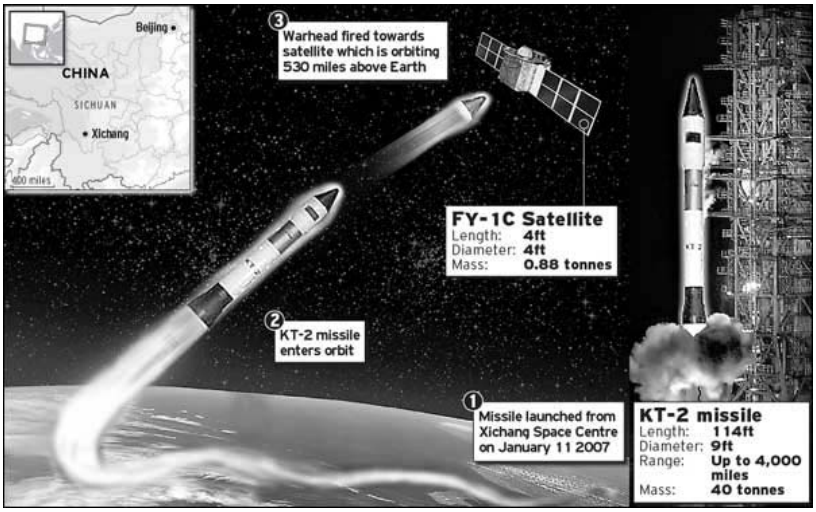

Figure 1 Chinese Anti-satellite Test[20]

Threats

Why the U.S. Has Fallen Behind

Until recently even those closest to developing, acquiring and operating our national space assets have deemed the threat to U.S. space systems as relatively low.[21] Credible threats existed during the Cold War from the Soviet Union's Anti-Satellite (ASAT) programs. Based on that threat, the U.S. conducted extensive work on developing countermeasures. The abrupt fall of the former Soviet Union and the subsequent end of the Cold War came without the need to execute our planned defenses[22], leaving many to question whether we ever needed them at all.[23] This built a mindset of complacency within the U.S. space community, and a feeling that any threat to our space systems was unrealistic and contrived. Clearly, many felt that the U.S. should focus its efforts internally instead of externally on what many believed to be a non-existent threat.

Starting in the late 1980s the U.S. channeled its efforts internally on the ever-difficult task of getting its space systems off the ground and into operations. The Space Shuttle disaster in 1986 complicated matters immensely taking away what had promised to be the new U.S. space heavy delivery system of choice.[24] Suddenly, the U.S. was without a reliable heavy delivery system.[25] The U.S. felt this void even more when it experienced several launch mishaps and disasters as it attempted to field an adequate launch system to take the place of the Space Shuttle.[26] Essentially, it appeared the U.S. had lost the magic of gaining access to space.

Over the next decade the U.S. increased its internal focus as it continued to rebuild an ailing launch capability. Such an undertaking required significant resources, and left little time to look externally at how enemy space control systems might be evolving. Worse yet, it left little time for the development of tactics, techniques or procedures (TTPs) to handle these potential threats. This meant the U.S. had given little thought as to how it would handle an attack on its systems.[27]

Just as the U.S regained confidence in its launch capability, U.S. space systems began to pay high dividends on global battlefields such as those during Operations DESERT STORM and ALLIED FORCE. As commanders began to understand the advantages gained from using space assets, the leaders who owned and operated these space systems put full effort into meeting these global warfighting needs.[28] Development of a Space Air operations Center (AOC) at 14th Air Force and a Space Tasking Order (STO) institutionalized the ways and means, within the Air Force, space would be integrated and synchronized into each theater of operations.[29] Again, this demanded tremendous focus and effort leaving little to advance comprehensive understanding of space threats and TTP development. Such a limited focus on protecting space assets could possibly be attributed to an assumption that space assets would be available for U.S. use regardless of who or what enemy systems the U.S. might engage.

What Caught the U.S.'s Attention?

In 2001, Donald Rumsfeld led a commission whose sole purpose was to take a detailed look at U.S. national security space management and organization. Known as the "Space Commission", Rumsfeld and his team presented what should have been the wake up call the U.S. needed, after having decades of atrophy to its space control efforts. In general, the report described both the U.S.'s reliance on its space assets as well as the vulnerability of these space assets to enemy attack.[30] The report went on to point out that it was not a matter of if, but rather when an attack would take place.[31]

Within the space community, many took note of the report but few took action to implement the Space Commission's proposals in a comprehensive manner.[32] At the time, the USAF spent considerable organizational effort toward integrating space effects into joint operations. These

efforts competed for resources and attention. Then, a sequence of events led many space leaders to shift their focus once again to space control.

The Space Shuttle Columbia disaster in 2003 was the first of these events. The investigation into the break up required the U.S. draw upon its space surveillance network, in hopes of gathering facts about the incident. In the process, more questions than answers where found. Therefore, the U.S. space community came to a deeper realization that its capacity to see and know what was happening in space was extremely limited. Although, in this instance, it was merely a matter of being unable to find a definitive reason for the disaster, many saw this lack of space situational awareness as an inherent weakness in U.S. space capabilities. A weakness in which, many feared, an adversary could take advantage.

Less than a year later, the U.S. State Department was having problems with its Voice of America broadcasts going into Iran. Specifically, an unknown source was jamming the transponder on the commercial communication satellite, TELESTAR 12, which the State Department leased for these broadcasts.[33] After a few weeks, the source of the jamming signals was isolated to a dish located on the Iranian Embassy's roof in Cuba.[34] The U.S. then issued a demarche to Iran, they removed the dish, and the jamming subsequently stopped.

Although the result was what the U.S. wanted, the way in which this event played out caused U.S. leaders much consternation. Upon discovery of the jamming signal, the U.S. realized it lacked effective means for handling such space control situations or any coherent methods for bringing a diverse group of space entities together for problem resolution. For example, the National Reconnaissance Office (NRO) owns all the space assets required for searching for ground generated jamming signals while United States Strategic Command (USSTRATCOM) owns the mission for space superiority.[35] Without a documented,

institutionalized, and practiced method of working together, it took these groups weeks instead of hours or minutes to pin point the source of the jamming. This left many to start asking what would have happened if the same thing had occurred to a space asset our warfighters rely on during times of crisis or war. Again, the event pointed to insufficiencies within the U.S. space control program since the end of Cold War. Just as the Space Commission had warned over six years ago, the U.S. remains unprepared for an attack of its space systems.

The Threat Today

The threat today stands in stark contrast to the one that the U.S. faced during the Cold War. Instead of facing a single super power, the U.S. now faces a spectrum of threats. These threats range from familiar state-actors to that of non-state actors or even individuals. The amount of activity to contest U.S. freedom of action in space is growing.[36]

China now stands on top of this growing list of threats to U.S. space assets.[37] Over the past several years, it has dedicated itself to growing its space and space control capabilities.[38] From conducting their first manned space launch in 2004 to a provocative direct-ascent ASAT demonstration in early 2007, China has been determined to show the world they are a rising space power.[39] Specifically, this ASAT testing involved launching a KT-2 missile and hitting one of their FY-1C weather satellites in Low Earth Orbit (LEO).[40] This action proved that they now have the capability to target satellites in LEO. Again, for the U.S. this means some of its most precious natural security assets, its intelligence satellites, are now within striking distance of a Chinese ASAT attack.

In addition to its ASAT weapons, the Chinese have also been hard at work developing directed energy space control weapons. For example, the Chinese have nearly perfected ground-based lasers with the capability to track and target on-orbit space assets. In September 2006, Dr.

Donald Kerr, the Director of the National Reconnaissance Office, confirmed the Chinese weapon "blinded" a U.S. reconnaissance satellite.[41] By doing so, the Chinese had been able to specifically find, fix, track, target, and place a laser with great precision on one of our spy satellites; essentially taking it momentarily out of operations by attacking it with directed energy.[42]

Such provocative steps are not limited to those states with enormous defense funding behind them. Many have described how to build Global Positioning Satellite (GPS) and mobile satellite communication jamming devices for around $7,500 or less.[43,44] Additionally, celestial observation technology, such as adaptive optics that help correct for atmospheric disturbance, have greatly declined in price so much that even casual astronomers can field a device for tracking and viewing U.S. satellites in LEO. Such capabilities, while benign on the surface, could potentially lead to an adversary being able to gain critical information on satellite construction, materials used, operating capabilities, and potential satellite vulnerabilities. For satellite communication jamming, countering U.S. capabilities could be as easy as building a system from only an electric generator, wood, plastic piping, and copper tubing to overwhelm any antenna or military receiver in the area.[45] By doing so, an adversary could deny the U.S. the benefits of these precious assets during the time they place this energy over the battlefield.

Non-state actors such as terrorists are sure to view space control systems as a method for big pay off against the U.S. with little effort or cost. Again, space control technologies are proliferating worldwide. It would appear that it is just a matter of time until these groups strike. The U.S. must take both these non-state as well as the traditional state powers in consideration when evaluating who might do their space systems harm.

U.S. Space Policy

U.S. space policy remains a two-sided coin. On one hand, the U.S. firmly states its intentions as those seeking peaceful purposes for the benefit of developing its civil, commercial, and national security interests.[46] On the other hand, the U.S. makes its intentions clear to preserve its rights, capabilities and freedom of action in space.[47] This dichotomy between peaceful aims while seeking to further its own self-interests has driven an air of uncertainty around the globe.

Many nations, particularly those in Russia and Europe, see this policy as a means to make space increasingly hostile.[48] In response, there are many nations looking to a future filled with hostility in space.[49] Much of the same rhetoric describing the U.S. military in general is now being applied to space assets and intentions. For decades, many viewed U.S. military policy as one offensive, aggressive in nature. With U.S. space policies clearly establishing our nation's intentions to seek growth and exploration in space, many now have this same impression regarding how the U.S. views space. This U.S. willingness to seek continued growth in space has left many fearing an impending arms race in that medium.[50] Such a space arms race might meet stiff opposition from our allies who are spending less and less on their militaries.[51] In addition, the price tag associated with developing space capabilities is so significant it limits the numbers of nations that are even able to participate. Such exclusion may create even more anxiety from those nations lacking the financial capability to participate in the space race.

Although this is true, the language within the U.S. space policy helps provide the necessary flexibility it will need when looking at an uncertain future. In the past, the U.S. has essentially claimed its right to act on others in space in terms of self-defense. This was seen as more of a quid pro quo type scenario involving retaliation based on an attack on U.S. systems. Recent

policy language makes it clear that the U.S. will not only respond in a manner reflecting self-defense, but also in terms of protecting its self-interests. What exactly this language will mean in terms of U.S. will and capabilities to act offensively remains unclear, but such language opens the door to seemingly justify the use of offensive action in space.

How Artificial Neural Networks Work

Technological progress is like an axe in the hands of a pathological criminal.

—Albert Einstein, letter to a friend, 1917

Neural networks are not a new concept. In fact, they have been around since 1943.[52] And, some might argue that these networks have been around since the beginning of time. After all, they are based on the biology of living things. Humans have neurons that when presented with an input or stimulus will fire or not fire depending on what that neuron has been taught in the past.[53] For example, if we put our hands on something hot, we get an immediate reaction to pull our hand away. Our brains have been wired or taught based on experience that something hot may cause damage and pain to us. So, to prevent this, our neurons have been taught to fire a pulse to move our hand away based on this level of pain tolerance.

Artificial Neural Networks (ANNs) work in this same manner. These ANNs have neurons arranged in a variety of layers to create a network. Each of these neurons will then fire or not based on a given stimulus. Network designers or autonomous operating networks determine the criterion for this action or inaction through examples called weights.[54] Weights act as a threshold that an input must cross in order for the neuron to take a given action. Again, this threshold is similar to the pain threshold we feel when placing our hand on something hot. Once

crossed, the neuron will fire, and an action will take place. This creates a flexibility not found in other types of networks or systems, like those run by computers, which must follow a list of instructions in order to solve a problem.[55] Neural networks, on the other hand, are able to constantly update themselves and learn as they encounter different situations through a process known as adaptive learning.[56] The adaptive learning process is the method in which a neural network builds its collective intelligence by experiencing, giving meaning, and remembering each situation as it occurs.[57] This enables the neural network to take the correct action should that situation arise in the future.

How Neural Networks Learn

Neural networks learn to take these correct actions based on the implementation of a few methods. The first of which is associative mapping. Associative mapping occurs when a neural network learns to recognize an input pattern and takes the appropriate action based on what it knows to do for that given pattern.[58] This recognition occurs through either auto-association, when an input exactly matches the pattern a neural network has learned in the past, or hetero-association, when the input is close to but not the exact pattern a neural network has learned in the past.[59] In the latter case, either the neural network will use a method called nearest-neighbor recall by looking at the input that most closely resembles something it has learned previously, or it will use a method called interpolative recall by taking the input data and using interpolation to generate the correct action.[60]

Another method through which neural networks learn is called regularity detection. Regularity detection differs from associative mapping in how it translates the input data. Again, in associative mapping, the neural network takes the input data and translates it into a pattern.[61] Regularity detection, on the other hand, translates the input data by giving it some form of

meaning.[62] By doing so, this method closely resembles how humans learn. In recalling the earlier example of when we touch something hot, our brain gives meaning to each experience in which a certain pain threshold is crossed. This meaning is stored and subsequently recalled when we experience similar events in the future. We are then able to take actions based on past experiences (e.g. move hand away quickly).

Variations in Neural Network Design

Similar to the different neural network learning processes, there are also differences in neural network design. One such design difference is the network's ability to change its weighting criteria. In a fixed network, the weighting or threshold for action or in action does not change.[63] This means that once a neural network begins to solve the problem at hand it will not update or adjust its weighting, and the threshold criteria it had in memory will stay consistent.[64] On the contrary, an adaptive network will change its weighting through out the problem solving process.[65] This allows the network to make adjustments to these action thresholds in real time as the problem is being solved, making it a much more precise and powerful tool.[66]

Another difference in network design is found when comparing feed-forward and feedback network designs. A feed-forward network allows an input signal to travel in only one direction.[67] The signal will continue forward based on whatever weight is associated to produce an action or inaction. Drawing on the previous example, if the input signal is heat on your hand then the output signal will be to move your hand once the heat becomes hot enough to cross the weight set pain threshold. While this is a simpler network design, it lacks the flexibility found in feedback networks. In feedback networks, the output signal not only moves forward like the feed-forward network, but also loops back to become an input again.[68] By doing so, these networks constantly update themselves until they reach a refined equilibrium point based on the

initial input.[69] Again, this makes the feedback network much more flexible with an ability to constantly update itself.

Neural networks also differ in design based on whether or not they are supervised or unsupervised. A supervised neural network involves the intervention of an external monitor into network operations.[70] This type of network will prompt the external monitor to enter the data into the network to give meaning to any input it has not seen prior to taking action. Such intervention can improve the network's performance because the external monitor has complete control over how the network will react to any given input. On the other hand, a negative ramification of this network design is that it may slow the network down because it must wait for the external monitor's input prior to taking action. Opposite of a supervised network, an unsupervised network will take action based on a given input autonomously.[71] To do so, an unsupervised network will use the processes discussed earlier regarding how neural networks learn. The benefit of these networks is their ability to operate at increased speeds because they do so without any external intervention, and are only limited by their computing speed. The downside of this network design hinges upon its performance. Without external monitoring the network is left to give meaning to inputs all by itself, which can lead to inconsistent performance. The reason for this inconsistency is directly tied to a network's ability or inability to perfectly identify what an input is, what action it must take based on this input, and its associated weighting criteria.[72]

Satellite Application

The use of neural networks on satellites seems like a match made in heaven. After all, the U.S. launches satellites into space with the hope that it never sees or touches them again. Each satellite needs to be without flaw when launched because there are few if any opportunities

to fix them once they are on orbit. The U.S. does its best to prepare satellites, put safeguards in place to protect their components, and then hopes for the best. Unfortunately, no system is perfect and the U.S. has yet to produce a perfect product. In fact, things such as destructive space weather effects, hardware failures, and other mishaps on orbit have often baffled the U.S.[73] Added to this complexity, satellites are often in operation for 10 plus years with the only way of caring for them being computer commands and software updates sent through the ether thousands of miles away. A lack of U.S. responsive launch capability exacerbates this complexity by preventing it from easily replacing these aging satellites.

Part of the current protection plan for these spacecraft is to place the most up-to-date computer hardware and software on-board. However, due to the aforementioned longevity, this combination is often obsolete shortly after launch. Added to this, it is extremely difficult and risky to update software while the satellite is in orbit. This restricts our ability to make the updates to them, which are essential in helping them adapt to a constantly changing environment.

Neural networks could decrease the difficulty associated with maintaining current software because they have the ability to learn continuously. Unlike standard computer software that remains stagnant until updated with a newer version, neural networks can adapt their behavior based on real-time experience and user input. Again, these networks attempt to mimic the behavior found in our own brains and their performance improves through leaning and experience. This capability would allow spacecraft to have the intelligence to act in the most efficient manner even as its capabilities and the external environment changes over time. For example, if a certain spacecraft component shuts down when it is exposed to radiation from charged particles, a neural network would learn from this and then learn how to take the appropriate actions necessary to avoid the shut down. Additionally, it would be able to do so

without numerous invasive and risky software overhauls. Over time, the risk avoided by not having to complete these software updates could be significant.

Neural networks also improve upon the "all or nothing" response produced by current spacecraft hardware and software when faced with an anomalous situation. This type of response occurs when a spacecraft's software receives an input outside of its normally programmed boundaries. The software will then trip safety measures to shut down what ever is affected by these out-of-bounds inputs. Once turned off, the spacecraft lacks the ability to turn on what ever it previously turned off. The logic behind this is that the spacecraft will put itself into a safe position and wait for ground operators to figure out what happened and how best to fix things. The problem with this method is that the spacecraft will be unable to operate until ground operator intervention occurs. Simply stated, this could be hours, days, or even weeks.[74] During this time, the effects provided by the spacecraft will be unavailable to those who desperately need them.

Neural networks offer a potential for vast improvement on this all or nothing response because they can handle inputs that are not merely within or outside of set boundaries by using interpolation. In other words, neural networks can handle inputs that are not black or white, but gray. This allows a spacecraft to respond effectively to a wider range of situations its software cannot handle, without merely turning off the effected systems. In essence, a neural network can essentially read between the lines during this uncertainty or gray area, and find the best response based on what it has been taught. In addition, since neural networks have the intelligence to understand what the input it receives means, it has the capability to not only turn things off when they are out of set bounds but also to turn things back on when they go back in. Again, this allows a neural network to work beyond the all or nothing response. In doing so, the neural

network can understand when the input that caused it to turn off a given system is no longer present, and can be taught to turn the system back on.

The flexibility that results from the ability to correctly identify what an input is, and to act autonomously based on learning, is the major advantage of using neural networks on spacecraft for defensive space control purposes. In attempting to maintain use of our space systems, the conditions must be set in which our systems stay online to produce the effects we desire. For a spacecraft, this means keeping its sensors and systems functioning regardless of the environment it's operating in. If attacked with some form of directed energy, hypothetically the neural network would correctly recognize what is happening based on its understanding of the input data, and would then take the actions the necessary to protect the spacecraft. Then, as the input data changes when there is no longer any directed energy placed on the spacecraft, the neural network will reverse the previous corrective actions to bring the spacecraft back into operation. Such action would significantly minimize the enemy's effects on our satellites, especially those in LEO. Again, instead of being out of operation for hours, days or weeks, a neural network would put the satellite back into operation as soon as the spacecraft moves out of the range of enemy systems. With the speed in which LEO spacecraft move over the earth, these neural networks might minimize spacecraft downtime to less than 15 minutes.

Challenges

Although neural networks represent an opportunity to improve a spacecraft's ability to protect itself, they also present significant challenges. Specifically, limitations in input data, spacecraft computing power for storage and processing capability, external monitor interface, performance unpredictability, and inherent spacecraft response shortfalls are all areas that need to be improved for neural networks to achieve their full potential on-board spacecraft.[75]

A neural network must have useful input data in order to perform effectively. Most people are familiar with the phrase "garbage in, garbage out." The same can be said with neural networks. On a spacecraft, the input data source comes from its telemetry or data readings generated from all its on-board systems. These readings give the spacecraft and ground operators an understanding of the spacecraft's performance. Although there are hundreds or thousands of these readings for any given spacecraft, there might not be enough or enough with the right fidelity to capture the data required for a neural network to determine whether or not an attack occurred. To mitigate this issue, a close examination of sensors types and their respective fidelity must take place in order for the neural network to operate as required.

Another challenge with neural networks is the lack of spacecraft computing power used for data storage capacity and processing. As previously discussed, input data comes from several spacecraft telemetry readings. Since these telemetry readings often number in the hundreds, and current spacecraft processors are limited in memory and power, they can usually only monitor a handful of the most critical readings (e.g. power, thrusters, and fuel). Neural network on-board spacecraft must contend with these same computing limitations. This is an issue because neural networks require tremendous data storage capacity and processing capabilities.[76] Like humans, neural networks must store, organize, and maintain their memory banks in order to draw upon them when attempting to correctly handle situations as they occur. With hundreds of telemetry readings requiring monitoring and storage, this will likely result in a strain on the spacecraft's memory capacity. Additionally, neural networks must have the ability to act upon this inputted telemetry data. This necessitates powerful processing speeds to rapidly sift through the vast amounts of stored telemetry readings.[77] Again, in order for an on-board neural network to

recognize it is being attacked and to take protective actions, these processing speeds must be measured in milliseconds, not minutes or hours.

To accommodate these computer memory and processing needs more powerful on-board computers will be needed. Depending on the number of telemetry readings a significant leap in computing power, while simultaneously shrinking the computer's size and power, is required.[78] In fact, to get to the point where neural networks have the same cognizant ability as a human, it is estimated that the necessary computing power is well over a decade away from being developed.[79] In addition, just like current spacecraft operations, the number of telemetry readings monitored and the frequency in which they are measured, can be adjusted to limit the memory required for storage and to compensate for limited processor speeds.[80]

The amount of user interface needed to ensure performance predictability is another challenge that must be overcome. As previously described, there are two types of neural network designs when it comes to user input into the network's performance: supervised and unsupervised networks.[81] The key difference between the two falls to who makes the decisions as to what the input data means, an external monitor or the network itself, and how this input effects network performance.[82] In order to achieve a point at which a neural network can make flawless decisions that will affect the entire spacecraft, an extensive training period will need to be conducted. This requires the external monitor, not the network itself, to manually input meaning into the network until the network is able to draw upon such stored meaning to correctly handle situations as they occur. The process to do so can take months to ensure the system is able to perform adequately, and will not make a mistake that could possibly put the spacecraft at risk (e.g. cause the spacecraft to tumble, lose contact with its ground station).[83]

The fact that spacecraft currently have limited protective and response measures is also a challenge. Spacecraft "fly" in predictable patterns over the earth with limited ability to maneuver. Such predictability in known patterns makes them easy targets for those wanting to attack. Regardless of how well an on-board neural network performs in identifying an attack, it may not be able to overcome the effects of the attack due to a lack of counter measures available on the spacecraft itself. With regard to a directed energy attack such as a laser or jamming, a neural network could have success in turning off or shielding vulnerable sensors and components. While this is true, a neural network would have very limited use against the launch of an anti-satellite weapon (ASAT) or a ground launched missile. Even if the spacecraft's sensors detected a kinetic ASAT launch, fed the launch data collected to the neural network correctly, and the neural network commanded the spacecraft to move properly, the spacecraft's orbit would bring it back over that very same spot less than two hours later. Those attacking the spacecraft could merely re-track and re-target the spacecraft for another opportunity. In addition, if the ASAT weapon has the ability to course correct in mid-flight it could possibly strike the spacecraft, no matter what the neural network did to move the spacecraft out of harm's way.

Possible Space Superiority Scenarios & Their Impacts on NN Design

Look before, or you'll find yourself behind.

—Benjamin Franklin

When attempting to manage an uncertain future, it is important to consider more than one alternative. Major Scott Maethner, in his research work entitled "Space Power – The Next 50 Years," used scenario planning to develop four possible alternative futures in order to help inform space superiority strategies. Specifically, he weighed the alternatives associated with the frequency of attacks on space assets and the strength of political will. The alternative realities

these variables provide have a distinct impact that could effect how neural networks are developed in the future.

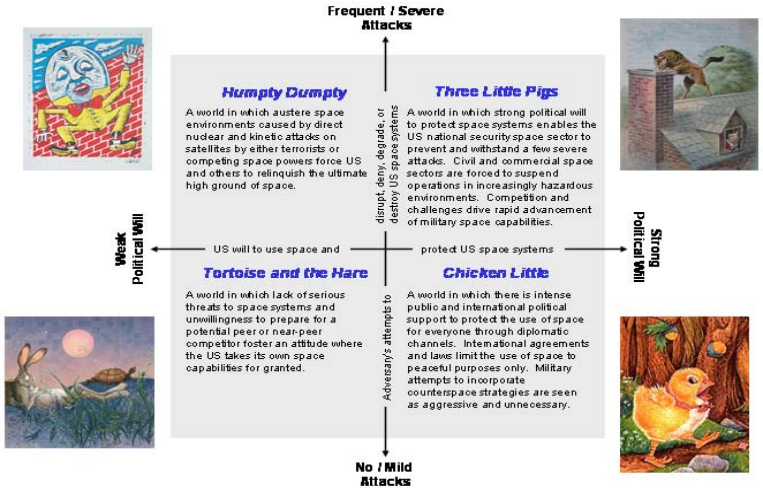

Figure 2 Maethner's Space Superiority Scenarios

Humpty Dumpty

The Humpty Dumpty future is one filled with adversaries attacking U.S. space systems while the U.S. chooses to do little about it.[84] The result of this future is one in which the U.S. relinquishes its space assets and backs away from space.[85] In looking at the four possible future alternatives in space, Humpty Dumpty truly represents one of the worst-case scenarios regarding the possibility of developing space control systems. Although adversarial attacks on U.S. space systems would justify a U.S. response, a weak political will would prevent this from occurring.

The Humpty Dumpty world would present challenges for those attempting to develop space control systems. Neural networks and other types of systems aimed at protecting U.S. space systems would be put on hold, as those in charge would walk away from military and government space assets. This would have a dramatic impact on funding and subsequent contracts for space control systems, and could potentially stall neural network development.

In the sense of what the U.S. government would be doing with its systems, such a future scenario would likely halt space control system development within the commercial sector as well. Despite the fact that space services are a profitable venture today, the Humpty Dumpty scenario illustrates an environment austere enough to force commercial space entities to shut down their efforts in space.[86] By doing so, the market for space control systems would likely come to a virtual standstill as commercial entities would stop spending on development of protection systems for assets they no longer use.

Three Little Pigs

The Three Little Pigs scenario presents an environment in which attacks are still occurring, yet unlike Humpty Dumpty, the U.S. chooses to protect its assets.[87] Additionally, it presents a situation in which civil and commercial entities suspend operations due to the extreme hazards involved in operating their systems in such a hostile environment.[88] In terms of developing neural networks and other space control systems aimed at protecting U.S. space systems, this alternative future represents a best-case scenario.

In such a situation, it is likely the U.S. will significantly increase its spending on defensive space control systems. This, in turn, should increase the likelihood of their successful development. In terms of a neural network used for protecting a LEO satellite, this scenario and environment of increased developmental spending represents its best chance. Again, an increased level of developmental focus and resource allocation is likely to lead to a better end product.

Tortoise and the Hare

The Tortoise and Hare scenario presents a future where there is no credible threat to the U.S.'s space systems.[89] Based on the lack of threat, the U.S. would not feel the need to prepare

for an attack on its space assets, and would therefore take its space systems for granted.[90] This alternative future truly represents the worst-case scenario for the development of space control systems. Without a legitimate threat to its space assets, or a perceived need to protect its systems, the U.S. would likely turn its focus and resources toward other more urgent interests. Essentially, this would have the potential of completely hampering DoD and Air Force neural network development for the purpose of defensive space control. Such an environment would stop this type of development until a relevant threat impacted the U.S. and/or the U.S. made the decision to protect its systems.

Chicken Little

The Chicken Little scenario presents a future in which the U.S. seeks the peaceful use of space through heavy political and diplomatic means on the international level.[91] Additionally, the world sees any development of space control systems and capabilities as being overly aggressive.[92] In looking at historical events and context this alternative future might be more appropriately entitled "The Romantic Past." While this alternative is meant to describe a possibility for the future, of the four possibilities, it is the one in which the world has slowly moved out of over the past several decades. Since it reflects the past, this scenario illustrates limited attention on space control system development and applications. This, in turn, would leave the U.S. where it is today with regard to neural network development. Simply stated, it would leave U.S. behind in developing these systems.

In addition to the conditions found in these four space superiority scenarios, two drivers could possibly effect the future development of NNs. These drivers include commercial market interest and the rise of non-state actors with a discussion of each found within Appendix C.

Conclusions and Recommendations

When you come to a fork in the road, take it.

—Yogi Berra

Operational Impact

The U.S. is more dependant on space than any other nation. Although the link between space assets and warfighting capabilities is the most publicized, space activities across all sectors (defense, intelligence, civil and commercial) are vital to U.S. national, economic, and homeland security. A contested space domain is a potential threat to vital U.S. interests.

On-board artificial neural networks offer one of many possible space control technologies to address protecting U.S. space assets from a variety of threats. By giving satellites the ability to identify what is attacking it and to take the action required to protect itself, the desired effect U.S. adversaries are aiming to inflict on the U.S. can be minimized. Essentially, a neural network will put the satellite in a protective mode to shield it from directed energy only during the duration of attack. In addition to protecting the satellite, such actions will also limit the time a satellite is out of operation to the amount of time that particular satellite is within view of what is attacking it. For a LEO satellite, this is a matter of mere minutes as it rapidly passes over an adversary's space control system location. This would be a huge leap forward from current satellite capabilities that basically turn a satellite off until ground operators intervene to fix and turn them back on. This process is often lengthy and may require a number of engineers many days to investigate the situation and return the system to normal operations. An on-board neural network capability that brings increased decision-making capability to a satellite would shorten this time and, possibly, even decrease the number of personnel necessary to handle these types of emergencies.

Recommendations

The U.S., in general, and the Air Force, in particular, should continue to develop neural networks and integrate them into its satellites. To do so the Air Force should continue its development of ground based neural networks, such as the Aerospace Corporation's Satellite as a Sensor (SAS). Specifically, as discussed in Chapter 1, the Air Force should continue to use SAS to monitor the daily operations of its spacecraft across various platforms, in order to train the system to delineate between what is normal satellite behavior and what is an anomaly. Once the Air Force fields SAS, it should conduct live fire ground or on-orbit testing using simulated direct energy attacks on one or more of its satellites. Currently, several satellites are out of operation and are being used as test beds for other activities. These would be perfect candidates to conduct such testing, in order to determine whether SAS could detect an attack through the particular satellite's telemetry. Once the Air Force conducts these tests, it should then be able to identify neural network performance shortfalls, as well as the data shortfalls from the satellite's telemetry and sensor inputs.

Once these tests are completed, the Air Force should then work to develop a neural network capable of being housed on-board a satellite. Such development is critical because SAS is a ground-based system that does not have to contend with the size, power, storage, and processing power limitations found on-board satellites. To do so, these variables must be considered while identifying performance trade-offs in order to produce a system that can be placed in a satellite. Additionally, "must have" performance parameters will not only need to be identified, based on this trade-off study, but also ensured they are placed into the system.

Once a feasible on-board neural network is developed, the Air Force will need to identify additional technology hurdles affecting neural network operations. Considerations such as:

satellite sensor technology and sensitivity, satellite processor capability, antenna bandwidth for links and nodes, and ground station architecture are essential for system success. Other considerations that must be closely examined are the architecture of possible host spacecraft, as well as current and future system interoperability such as the Rapid Attack Identification Detection Reporting System (RAIDRS) or the Space Based Radar (SBR). As discussed in Appendix B, this interoperability will enable a variety of systems to share data and improve each system's overall SSA.

In addition to system considerations, the Air Force must examine its current space decision-making culture. Currently, the decision making process within the Air Force's space community is extremely hierarchal and stove piped. In other words, to reconfigure or fix a broken spacecraft, the decision/plan to do so will require approval from multiple levels of management. This process is slow and tedious, and often creates unnecessary delays in bringing a satellite back into operation. Furthermore, strict security enclaves prevent information cross-flow. This culture must change in order to fully utilize the potential of a neural network or any system that has the capacity to make man-out-of-the-loop decisions (or increase machine to machine contacts) and actions. In order to build confidence in their ability to perform appropriately, rigorous testing of these kinds of systems is necessary prior to bringing them on-line. If over concerned leadership or ground operators hamper these systems, they will never be able to achieve their rapid response capability.

On-board neural networks have the potential of giving the U.S. and the Air Force a means of protecting some of their most valued assets in space. For this reason, it is critical the Air Force considers these recommendations. If the Air Force fails to do so, it may find itself fighting without the benefit of space assets at a time and place it can least afford to do so. Although such

warnings seem somewhat overstated, considering the threat environment U.S. and Air Force space assets currently operate in, such statements are not without foundation when examining history. After all, who could have predicted the full impacts associated with technological breakthroughs such as the airplane or GPS? In each case, those who sought to utilize them found themselves at a significant advantage in battle. The fact remains, no one can predict the future. Instead, we should consider the possibility of different future alternatives and trends, while using the past as a guide when its context is applicable. The U.S. and the Air Force only need to look as far as the intersection of future technological growth and that of an ever-immerging threat environment in space, to understand what the future will hold. While this may be an oversimplification of a problem gaining in complexity, the U.S. and the Air Force should act now to ensure they are ahead, not behind, this evolution.

Appendix A

Methodology

The crux of this paper is the attempt to look at the operational environment approximately 25 years into the future, and identify today's emerging technologies that the Air Force should invest in to maintain superiority within that environment. This process of attempting to understand and predict what will occur in the future, with regard to technology, is called technology forecasting.[93].

Technology forecasting has been around for centuries, but has come into its own when applying its methods towards economics and warfare. From an economics aspect, which technology will help me develop the widget that will make me the most money? For the military, which technologies will give me a decisive advantage in future armed conflict? Either perspective will push the person forecasting to grapple with the uncertainties involved with the future. Such uncertainties include: the feasibility of a particular technology, the availability of relevant data surrounding the specific technology, the amount of resources being applied toward technology development, political and public support, similar technologies already in existence, and the number of variables facing the development of the technology.[94]

With these vast differences between technologies and the uncertainty involved in predicting their future success or failure, it would stand to reason that no one method of forecasting can be applied in all cases. Rueuvan Levary and Dongchui Han outline eleven different methods[95]. These methods range from the Delphi method used to gain expert opinion through polling to that of scenario writing to explore alternative versions

of the future.[96] Again, while no one method works best for all cases, each of these methods do lend themselves to working better than others, given certain situations. Such considerations, as to the availability of experts in the particular technological field or the quality of information available, are just a few that will help decide which method best fits a given situation.[97]

Although several methods such as Delphi would have been adequate when developing this paper's topic, the availability of existing scenarios relating to future space environments made scenario based forecasting an easier choice. Specifically, the work of Scott Maethner, in his paper entitled "Space Power – The Next 50 Years," outlines four credible alternatives describing the potential future based on the variables of frequency/severity of attacks on space systems as well as the strength of the political will of those attacked. These factors are the basis on which I will examine how alternative futures might effect the development of neural networks on-board LEO spacecraft.

Appendix B

Further Research

Due to the limited scope of this research paper, a few areas of study still need to be closely examined. In particular, space system links and nodes should be studied in order to further understand how improvements in each could better protect U.S. space systems from attack. This research paper is solely focused on the spacecraft element of the total space system, but the links and nodes elements are often the most vulnerable to attack.

Additionally, further research should be conducted on the potential interaction between neural network development and the development of other DoD systems. Specifically, system development in the area of space situational awareness tools would greatly enhance the performance of a neural network by increasing the amount and quality of data fed into it. Such data would enable the neural network to learn and adapt to the most current operating environment because it would come from multiple sources, with multiple capabilities, instead of just a single spacecraft's telemetry. In addition to accepting data, the neural network could also be a potential data feeder back to the same situational awareness tools. Since these tools will be reliant on the amount of sensors feeding into them, neural networks have the potential to enhance these tools by giving them more data and more sources of data. But, unlike other sources feeding situational awareness tools raw, unprocessed data, neural networks will be able to feed these tools information it has already identified, categorized, and acted upon. By doing so, neural networks will theoretically increase the speed and accuracy of these situational awareness tools because they have already completed the data processing legwork in advance.

One final area of research that would enhance neural network development is a further study of the commercial sector's use of this technology. Since this technology has numerous commercial applications, it stands to reason that the private sector will develop neural networks at a more rapid pace than the military. Fully understanding these developments will enable the U.S. military to look for opportunities to leverage off of this work in pursuit of its own systems.

Appendix C

Impact of Commercial Markets and Non-State Actors

In addition to the four possible space superiority scenarios discussed in Chapter 4, two other drivers could possibly effect the future development of NNs. These drivers are commercial market interest and the rise of non-state actors.

Commercial Market Interest

Commercial interest can dramatically influence the growth of any technology. The same is true with regard to the possible development of neural networks. Commercial applications of neural networks have grown significantly with the use of more and more of these networks in place of humans.[98] In fact, these NN commercial applications have recently evolved to the point where they now perform tasks once requiring a human expert.[99] These tasks range from advising and forecasting to monitoring and tutoring.[100] As discussed earlier, neural networks have the ability to learn as they operate. Based on this learning, these networks evolve in their capabilities to make both simple and complex decisions. With this evolution of more capable networks, the amount of accuracy gained from these systems has improved.

The growing capability of these networks has not been lost on commercial entities. With the increasing cost associated with hiring and retaining personnel to do mundane tasks, neural networks offer the commercial market a profitable alternative. One area of neural network application that has grown in recent times is that of the dial-in customer service assistant.[101] Who has not encountered one of these systems upon dialing a 1-800 number when seeking help or some form of information? Having a computer system that

has the ability to answer a majority of calls of inquiry enables companies to cut the number of personnel required to do the same tasks while, at the same, increasing productivity. Neural networks achieve this because barring some computer system crash they are always available, can take a greater volume of calls simultaneously, and never call in sick.[102]

As commercial markets become increasingly competitive, companies will continue to look for methods of cutting costs. Again, neural networks provide an avenue to do just that.[103] Such interest in this form of technology will only enable neural networks to continue to advance, and will likely benefit the military sector as well. This very fact makes it probable that the commercial sector will continue to drive advances in neural network technology, and the military should be prepared to leverage off these technological and cost saving gains.

Rise of the Non-State Actor

The world continues to contend with the growing threats associated with non-state actors. Although the term non-state actor can describe such legitimate, non-violent groups as non-government organizations (NGOs) and multinational corporations (MNCs), the threat mentioned above revolves around illegitimate, violent non-state actors found in terrorist, insurgent, and paramilitary groups. As terrorist groups have grown from being able to only impact regional affairs to being able to strike nearly anywhere at any time, states will continue to search for the means to defeat them. Such attacks now find footing in sea, air, and cyberspace when previously they were limited to land. The attack on the U.S.S. Cole, the growing number of U.S. helicopters shot down in Iraq, the use of commercial aircraft to strike targets during 9/11, and their use of the internet for

recruiting and information operations prove these terrorists are looking to strike within the additional mediums of sea, air, and cyberspace.

Based on this movement into other non-land mediums, the next logical evolution of such attacks would be those directed at U.S. space assets. With the ability to inflict a maximum amount of damage using modest technology and expertise, a space-focused attack is potentially a draw for terrorists. An increase in such activity would likely fuel U.S. interest in developing its space control systems in order to protect these precious assets. Again, such focus would result in development of resources, contracts, and effort aimed at producing systems to protect U.S. satellites. Specifically, neural networks could benefit significantly from such focus, and may have their effectiveness and capabilities grow at an increased rate. While this is true, this growth would still depend on whether or not these non-state actors could organize to the point of being able to launch successful attacks on U.S. space systems. In other words, will these non-state actors become dangerous enough for U.S. decision makers to consider them a legitimate threat, and feel compelled to take action against them?

Glossary

ACSC	Air Command and Staff College
AF	Air Force
ANN	Artificial Neural Network
AOC	Air and Space Operations Center
ASAT	Anti-satellite
AU	Air University
AWC	Air War College
DOD	Department of Defense
GEO	Geosynchronous Earth Orbit
GPS	Global Positioning System
LEO	Low Earth Orbit
MNC	Multi-national Corporation
NASA	National Aeronautics and Space Administration
NGO	Non-government Agency
NN	Neural Network
NRO	National Reconnaissance Office
RAIDRS	Rapid Attack Identification Detection Reporting System
SAS	Satellite as a Sensor
SBR	Space Based Radar
SSA	Space Situational Awareness
STO	Space Tasking Order
TTPs	Tactics, Techniques, and Procedures
US	United States
USAF	United States Air Force
USS	United States Ship
USSTRATCOM	United States Strategic Command

Bibliography

Ahern, Dave. "Senator urges funding space-based satellite defense." *Defense News*, January 31, 2007.

Air Force Doctrine Document (AFDD) 2.1-9. *Targeting*. Department of Defense, 2006. Available online at https://www.doctrine.af.mil.

Air Force Doctrine Document (AFDD) 2.2-1. *Counterspace Operations.* Department of Defense, 2004. Available online at https://www.doctrine.af.mil.

"Backyard satellite jammers concern US Airforce." *Australian Broadcasting Corporation*. Available online at https://www.abc.net.au/science/news.

Beason, Doug. *The E-Bomb: how America's new directed energy weapons will change the way future wars will be fought*. Da Cap Press, 2005.

Behrens, Carl E. "Space Launch Vehicles: Government Activities, Commercial Competition, and Satellite Exports." *Congressional Research Service*, March 20, 2006, 1-16.

Berube, David M. *Nano-Hype: The Truth Behind The Nanotechnology Buzz*. Prometheus Books, 2006.

Brachet, G. and B. Deloffre. "Space For Defence. A European Vision." *Space Policy* 22, May 2006, 92-99.

Brewin, Bob. "Homemade GPS jammers raise concerns." *Computerworld.com*, January 17, 2003.

Carafano, James Jay. "Missions, Responsibilities, and Geography: Rethinking How the Pentagon Commands the World." The Heritage Foundation, August 26, 2004.

Carter, Tom. "Castro regime jamming U.S. broadcasts into Iran." *Washingtontimes.com*, July 15, 2003.

"China jamming test sparks U.S. satellite concerns." *Reuters.com*, October 5, 2006.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Indexed edition. Princeton, NJ: Princeton University Press, 1989, 372.

"Commission to Assess United States Nation Security Space Management and Organization –Final Report." 2001.

DARPA Neural Network Study, October 1987-February 1988. AFCEA International Press, 1988.

de Selding, Peter B. "French Government Wants Europe to Join 2nd Space Race. *Space.com*, February 12, 2007.

Fernandez, Adolfo J. "Military Role in Space Control: A Primer." *Congressional Research Service*, September 23, 2004, 1-16.

Frederick, Missy. "Sensor Web to Link Scientists to Remote Alaskan Sites." *Space News*, July 10, 2006, 16.

Gallant, Stephen I. *Neural network learning and expert systems*. Cambridge, Mass: MIT Press, 1993.

Garreau, Joel. *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies – and What It Means To Be Human*. Doubleday, 2005.

Hall, J. Storrs. *Nanofuture: What's Next For Nanotechnology*. Prometheus Books, 2005, 207-212.

Harden, Toby and Alex Massie. "Chinese missile destroys satellite in space." *Telegraph.co.uk*, January 19, 2007.

Hobbs, David. *Space Warfare: "Star Wars" Technology Disgrammed and Explained*. Prentice Hall Press, 1986.

Kurzweil, Ray. *The Singularity Is Near: When Humans Transcend Biology*. Penguin Group, 2005.

Kyl, Jon. "China's Anti-Satellite Weapons and American National Security." The Heritage Foundation, January 29, 2007, 6-7.

Lambeth, Benjamin S. *Air Power Against Terrorism: America's Conduct of Operation Enduring Freedom*. Santa Monica, CA: RAND, 2005, 277-280.

Levary, Rueuvan and Dongchui Han. "Choosing a Technology Forecasting Method." IM, January/February 1995.

Long, Teresa W. "Autonomous neural control of space platforms." USAF Phillips Laboratory, 1994, 2-14.

Lorber, Azriel. *Misguided Weapons: Technological Failure and Surprise on the Battlefield*. Brassey's Incorporated, 2002, 33-34.

Maethner, Scott R. "Space Power – The Next 50 Years." *Air University*, April 2005.

Muradian, Vago "China Attempted To Blind U.S. Satellites With Laser." *www.DefenseNews.com*

Oberg, James. "An outer-space war of words escalates." *MSNBC.com*, November 10, 2006.

Siganos, Dimitrios. "Why neural networks." *Imperial College of London Surprise 96 Journal*, vol 1. http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol1/ds12/article1.html

Siganos, Dimitrios and Christos Stergiou. "Neural Networks." *Imperial College of London Surprise 96 Journal*, vol 4. http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html

Sprenger, Sebastian. "Shelton: Space Warfare is Certain; DoD Must Get Ready." *News from Inside the Pentagon*, March 1, 2007.

Stergiou, Chris. "What is a neural networks." *Imperial College of London Surprise 96 Journal*, vol 1. http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol1/cs11/article1.html

Tschan, C.R. and C.L. Bowman. "Development of the Defensive Counterspace Test Bed (DTB), Volume-1, Sensors and Detection." *AEROSPACE Report Number TOR-2004 (1187)-2*, September 1, 2004.

"United States National Space Policy." 2006.

Ward, David G., R. Barron, R. Bird, J. Monaco, and Y. Well. "*Neural network flight control system*." Wright Laboratory, 1996, 1-35.

Notes

[1] Siganos, Dimitrios and Christos Stergiou. "Neural Networks." *Imperial College of London Surprise 96 Journal*, vol 4, 1. http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html

[2] Ibid.

[3] Ibid.

[4] In fact, according to Moore's Law, this power may continue to double every 18 months.

[5] The "kill chain" is a method used to prosecute joint operations against Time Sensitive Targets (TSTs). It includes phases associated with finding, fixing, tracking, targeting, engaging, and assessing these targets.

[6] Air Force Doctrine Document (AFDD) 2.1-9. *Targeting*. Department of Defense, 2006. Available online at https://www.doctrine.af.mil.

[7] Lambeth, Benjamin S. Air Power Against Terrorism: America's Conduct of Operation Enduring Freedom. Santa Monica, CA: RAND, 2005.

[8] "Commission to Assess United States Nation Security Space Management and Organization –Final Report." 2001.

[9] Space superiority is the freedom from attack that ensures our space platforms can continue to provide our air, sea, and land forces the space enhancement necessary for optimal force employment (AFDD 2-2.1, p. 3)

[10] "Commission to Assess United States Nation Security Space Management and Organization – Final Report." 2001.

[11] Muradian, Vago "China Attempted To Blind U.S. Satellites With Laser" *www.DefenseNews.com*

[12] "Commission to Assess United States Nation Security Space Management and Organization – Final Report." 2001.

[13] Air Force Doctrine Document (AFDD) 2.2-1. *Counterspace Operations.* Department of Defense, 2004. Available online at https://www.doctrine.af.mil.

[14] Ibid.

[15] Siganos, Dimitrios and Christos Stergiou. "Neural Networks." *Imperial College of London Surprise 96 Journal*, vol 4, 1. http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html

[16] Ibid.

[17] Ibid.

[18] Tschan, C.R. and C.L. Bowman. "Development of the Defensive Counterspace Test Bed (DTB), Volume-1, Sensors and Detection." *AEROSPACE Report Number TOR-2004 (1187)-2*, September 1, 2004, viii.

[19] Ibid.

[20] Harden, Toby and Alex Massie. "Chinese missile destroys satellite in space." *Telegraph.co.uk*, January 19, 2007.

[21] Sprenger, Sebastian. "Shelton: Space Warfare is Certain; DoD Must Get Ready." *News from Inside the Pentagon*, March 1, 2007, 1.

[22] Including the dismantling of intelligence gathering efforts vital to Space Situational Awareness

[23] Ibid, 2.

Notes

[24] "Commission to Assess United States Nation Security Space Management and Organization –Final Report." 2001, 17.
[25] Ibid.
[26] Behrens, Carl E. "Space Launch Vehicles: Government Activities, Commercial Competition, and Satellite Exports." *Congressional Research Service*, March 20, 2006, 2.
[27] "Commission to Assess United States Nation Security Space Management and Organization –Final Report." 2001, 17-18.
[28] Lambeth, Benjamin S. Air Power Against Terrorism: America's Conduct of Operation Enduring Freedom. Santa Monica, CA: RAND, 2005, 274-80.
[29] Ibid.
[30] "Commission to Assess United States Nation Security Space Management and Organization –Final Report." 2001, 99.
[31] Ibid, 18.
[32] Kyl, Jon. "China's Anti-Satellite Weapons and American National Security." The Heritage Foundation, January 29, 2007, 6-7.
[33] Carter, Tom. "Castro regime jamming U.S. broadcasts into Iran." *Washingtontimes.com*, July 15, 2003.
[34] Ibid.
[35] Carafano, James Jay. "Missions, Responsibilities, and Geography: Rethinking How the Pentagon Commands the World." The Heritage Foundation, August 26, 2004.
[36] "Commission to Assess United States Nation Security Space Management and Organization –Final Report." 2001, 18-20.
[37] Ahern, Dave. "Senator urges funding space-based satellite defense." *Defense News*, January 31, 2007, 1.
[38] Muradian, Vago "China Attempted To Blind U.S. Satellites With Laser." *www.DefenseNews.com*, 1.
[39] In fact, their ASAT testing involved launching a KT-2 missile and hitting one of their FY-1C weather satellites in Low Earth Orbit (LEO).
[40] Harden, Toby and Alex Massie. "Chinese missile destroys satellite in space." *Telegraph.co.uk*, January 19, 2007, 1.
[41] "China jamming test sparks U.S. satellite concerns." *Reuters.com*, October 5, 2006, 1.
[42] Ibid.
[43] "Backyard satellite jammers concern US Airforce." *Australian Broadcasting Corporation*. Available online at https://www.abc.net.au/science/news.
[44] Brewin, Bob. "Homemade GPS jammers raise concerns." *Computerworld.com*, January 17, 2003.
[45] Backyard satellite jammers concern US Airforce." *Australian Broadcasting Corporation*. Available online at https://www.abc.net.au/science/news.
[46] "United States National Space Policy." 2006, 1.
[47] Ibid.
[48] Oberg, James. "An outer-space war of words escalates." *MSNBC.com*, November 10, 2006, 1.
[49] Ibid, 2.
[50] Ibid, 3.

Notes

[51] de Selding, Peter B. "French Government Wants Europe to Join 2nd Space Race. *Space.com*, February 12, 2007.

[52] Siganos, Dimitrios and Christos Stergiou. "Neural Networks." *Imperial College of London Surprise 96 Journal*, vol 4, 1. http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html
[53] Ibid.
[54] Gallant, Stephen I. *Neural network learning and expert systems*. Cambridge, Mass: MIT Press, 1993, 1.
[55] Siganos, Dimitrios and Christos Stergiou. "Neural Networks." *Imperial College of London Surprise 96 Journal*, vol 4, 1. http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html
[56] Ibid.
[57] Ibid, 3.
[58] Ibid, 11.
[59] Ibid, 12.
[60] Ibid.
[61] Ibid, 11.
[62] Ibid, 12.
[63] Ibid.
[64] Ibid.
[65] Ibid.
[66] Gallant, Stephen I. *Neural network learning and expert systems*. Cambridge, Mass: MIT Press, 1993, 17.
[67] Siganos, Dimitrios and Christos Stergiou. "Neural Networks." *Imperial College of London Surprise 96 Journal*, vol 4, 9. http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html
[68] Ibid.
[69] Ibid.
[70] DARPA Neural Network Study, October 1987-February 1988. AFCEA International Press, 1988, 61.
[71] Ibid.
[72] Siganos, Dimitrios and Christos Stergiou. "Neural Networks." *Imperial College of London Surprise 96 Journal*, vol 4, 13. http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html
[73] "China jamming test sparks U.S. satellite concerns." *Reuters.com*, October 5, 2006, 1.
[74] Sprenger, Sebastian. "Shelton: Space Warfare is Certain; DoD Must Get Ready." *News from Inside the Pentagon*, March 1, 2007, 2.
[75] DARPA Neural Network Study, October 1987-February 1988. AFCEA International Press, 1988, 35.
[76] Tschan, C.R. and C.L. Bowman. "Development of the Defensive Counterspace Test Bed (DTB), Volume-1, Sensors and Detection." *AEROSPACE Report Number TOR-2004 (1187)-2*, September 1, 2004, 71.
[77] Ibid, 74.

Notes

[78] DARPA Neural Network Study, October 1987-February 1988. AFCEA International Press, 1988, 35.
[79] Garreau, Joel. Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies – and What It Means To Be Human. Doubleday, 2005, 100-01.
[80] Tschan, C.R. and C.L. Bowman. "Development of the Defensive Counterspace Test Bed (DTB), Volume-1, Sensors and Detection." *AEROSPACE Report Number TOR-2004 (1187)-2*, September 1, 2004, 73.
[81] DARPA Neural Network Study, October 1987-February 1988. AFCEA International Press, 1988, 61.
[82] Siganos, Dimitrios and Christos Stergiou. "Neural Networks." *Imperial College of London Surprise 96 Journal*, vol 4, 13.
http://www.doc.ic.ac.uk/~nd/surprise_96/journal/vol4/cs11/report.html
[83] Tschan, C.R. and C.L. Bowman. "Development of the Defensive Counterspace Test Bed (DTB), Volume-1, Sensors and Detection." *AEROSPACE Report Number TOR-2004 (1187)-2*, September 1, 2004, 70.
[84] Maethner, Scott R. "Space Power – The Next 50 Years." *Air University*, April 2005, 17.
[85] Ibid.
[86] Ibid
[87] Ibid.
[88] Ibid.
[89] Ibid.
[90] Ibid.
[91] Maethner, Scott R. "Space Power – The Next 50 Years." *Air University*, April 2005, 17.
[92] Ibid.
[93] Levary, Rueuvan and Dongchui Han. "Choosing a Technology Forecasting Method." IM, January/February 1995, 14.
[94] Ibid.
[95] Ibid
[96] Ibid, 15.
[97] Ibid.
[98] Gallant, Stephen I. *Neural network learning and expert systems*. Cambridge, Mass: MIT Press, 1993, 258.
[99] Ibid, 256.
[100] Ibid.
[101] Ibid.
[102] Ibid, 258.
[103] Ibid.