2013 5th International Conference on Cyber Conflict
K. Podins, J. Stinissen, M. Maybaum (Eds.)
2013 © NATO CCD COE Publications, Tallinn

Complexity and Emergence in Ultra-Tactical Cyberspace Operations

Jeffrey L. Caton
President
Kepler Strategies LLC
Carlisle, Pennsylvania, U.S.A.
Jeff.Caton@keplerstrategies.com

Abstract: This paper explores how the concepts of complexity and emergence can affect cyberspace operations that occur beyond human perception and intervention, such as automated cyber attack responses. It first introduces the concept of the ultra-tactical as an additional realm of operations in the traditional strategic-operational-tactical framework. The context of this realm is compared to human cognitive processes as well as machine processes used to aid human decision making. Potential biases intrinsic in both processes are identified and evaluated. Factors that contribute to the complexity of cyberspace environment in ultra-tactical time scales are reviewed and the potential impact of emergent events on automated decision making protocols are examined. Futuring methodologies are used to develop feasible operational scenarios which are in turn used to evaluate the benefits and risks inherent in implementing automated responses that operate without human cognitive interaction. Specific focus of the analysis includes determining if automated responses will be robust enough to accommodate the dynamic nature of cyberspace and if they can differentiate adversarial threats from natural emergent behavior.

Keywords: *complexity, emergence, automated response, futuring scenarios*

The views expressed are those of the author and do not necessarily reflect official policy or position of any Department or Agency within the U.S. Government. All information and sources for this paper were drawn from unclassified material.

1. INTRODUCTION

In an October 2012 speech, U.S. Secretary of Defense Leon Panetta [1] warned of a potential "cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life." To guard against such a catastrophe, he called for "common, real-time understanding of the threats in cyberspace" concluding that "after all, we need to see an attack coming in order to defend against that attack." This statement implies, perhaps unintentionally, that such cyberspace operations will follow the timelines of commanders in the traditional physical domains. However, attacks in cyberspace can occur in timescales measured in nanoseconds. This paper explores how the concepts of complexity and emergence can affect such cyberspace operations that occur beyond human perception and intervention, such as automated cyberspace defense and attack responses.

2. THE ULTRA-TACTICAL ENVIRONMENT

General Keith Alexander, Commander, U.S. Cyber Command [2] in his 2012 Congressional testimony highlighted the need for the U.S. military to have a "pro-active, agile cyber force that can 'maneuver' in cyberspace at the speed of the Internet." In his 2013 testimony [3], he mentioned that the inter-agency and international exercise CYBER FLAG "introduced new capabilities to enable dynamic and interactive force-on-force maneuvers at net-speed."

But how does one characterize and codify operations at such speeds? A useful model is one that expands the operational realm of cyberspace—the "network speeds"—as part of a more traditional framework. In this case, let us define the ultra-tactical environment as an expansion of the tactical portion of the traditional tactical-operational-strategic operations model.

Consider a one-second timeframe and some illustrative physical events that occur within it (Figure 1). The time required for this page to be processed from your retina to your frontal lobe is about 25 milliseconds. Light will traverse the Earth's equator in 130 milliseconds, during which time an M-4 carbine projectile will travel about 110 meters. Your average eye blink takes about 350 milliseconds. For cognitive processes, a Chess Grand master will discern danger from an opponent's move in about 650 milliseconds--this value represents an approximate threshold for the ultra-tactical environment [4].

Clearly in the ultra-tactical realm are processes and events that occur well below one second. This includes CPU processing speeds (GHz/nanoseconds), memory access, and hard drive seek times. On the opposite end of scale are macro processes

and events that are well above one second. These include activities that require deliberate cognitive processes for decision making, such as intelligence assessment, course of action development, and at the further reaches, policy development. Thus, the actual implement of cyberspace operations occur mostly in the realm below that which humans can comprehend. Certainly, this is an assertion that motivates many security professionals to develop defensive—and perhaps offensive—tools that function automatically in cyberspace. What implications are there for such automated processes occurring in this ultra-tactical realm?

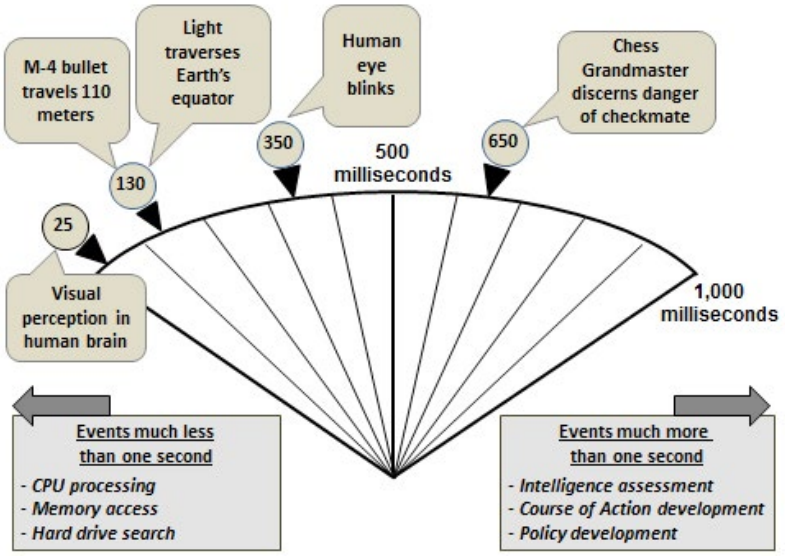

Figure 1. Typical events occuring within one second

3. CONTEXTS OF COMPLEXITY AND EMERGENCE

Geers [5] describes the dynamic nature of cyberspace as an environment where "insurmountable obstacles and golden opportunities can appear and disappear as if by magic." The flow of data occurs across nodes that may exist and disappear within fractions of milliseconds based on internal model attributes that prescribe a desired endstate (such as a software update). He proposes a codification of this phenomenon as one of the ten distinctive aspects of the cyber battlefield framework – specifically, "frequent software updates and network reconfiguration change Internet geography unpredictably and without warning." What are the factors that

contribute to the complexity of cyberspace environment in ultra-tactical time scales and what are the potential impacts of emergent events on automated operations to include decision making protocols?

Czerwinski [6] describes seven basic attributes of complex adaptive systems (properties: aggregation, nonlinearity, flows, and diversity; and mechanisms: tagging, internal models, and building blocks) and he argues that their interactions are fundamental to national security processes and warfare. *Aggregation* relates to the emergence of complex large-scale features from the interactions of less complex agents. *Tagging* facilitates formation of the aggregation by providing agents with traits that can be used for filtering. *Flows* relate to the development of networks among agents that are dynamic in scope as well as in adaption to appearing and disappearing nodes. *Diversity* relates to complex systems creating or fostering communities of agents "marked by perpetual novelty." *Internal models* give systems "the power to anticipate" using two model types: *tacit* which aim for implicit prediction of desired future state, and *overt* for explicit exploration of alternatives.

In sum, one can argue that cyberspace writ large is becoming more like a force of nature than a controlled and predictable network, especially in the ultra-tactical realm. As with the traditional physical domains, what humans are able to perceive and comprehend are manifestations of synergistic trends, properties, and characteristics of an infinitely dynamic environment. What are some of the implications of structure, scale, commonality, and diversity in cyberspace ultra-tactical environment?

A. BLACK SWANS AND DRAGON-KINGS

Emergent events based on models of the micro system dynamics that occur in the ultra-tactical realm may produce macro behaviors through self-organization and synchronization. Sornette [7] studied the dynamics of systems with large numbers of mutually interacting parts, specifically looking for mechanisms of self-organization that may produce surprising emergent behavior at the macroscopic level. In general terms, events that are statistical outliers with novel behavior are often referred to as "Black Swans" which tend to form in regions of self-organized criticality based on the degree of heterogeneity and interaction strength among the parts involved (see Figure 2). They are statistically expected, but not discretely predictable. The concept of Dragon-Kings refers to the existence of transient organization into extreme events that are statistically and mechanically different from their smaller siblings. They may be catastrophic events resulting from the strong coupling of highly homogenous parts in a complex system, and they do not need large perturbations to occur.

Examples of these phenomena are found in natural studies, such as organism networks and ecology in biology; plate-tectonics and erosion in geology; as well as applications in social sciences and economy. Unfortunately, Sornette concludes that "extreme events occur much more often than would be predicted or expected from the observation of small, medium, or even large events." How can this apply to cyberspace operations?

To be prudent, we should address certain ultra-tactical security measures that may drive macro behavior in cyberspace toward the Dragon-King realm. Specific examples include measures that push for increased system homogeneity and predictable interaction, such as: standardized desktops and intrusion detection systems; centralized networks; limited input/output portals; and automated responses. Geer and others [8] argued over a decade ago in their controversial report on Microsoft that use of a "single, dominant operating system in the hands of all end users is inherently dangerous" and that this danger is "exacerbated by tight integration between applications and operating systems." Their methods and findings are consistent with the Dragon-King characteristics of homogeneous systems that are tightly coupled.

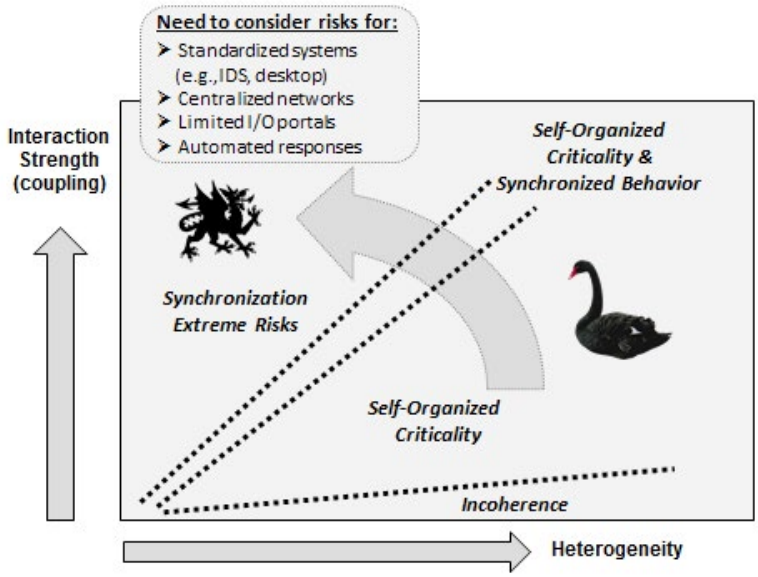

Figure 2. Conceptual emergent behavior

When considering the benefits of activities such as interoperability and cloud computing, we also need to balance the risks. This requires examination of risks posed not only by the threat vectors that these measures may open (or close) to a cognitive adversary, but also those environmental and design threats posed by the self-organization and synchronization they may introduce into the system. Of particular concern are unanticipated and undesired results emerging from ultra-tactical processes to support human situational awareness and decision making.

B. COUPLING IN COMMAND SYSTEMS

Geers [9] characterizes attack and defense in cyberspace as a "game of cat-and-mouse" since over time the opposing forces will develop complex algorithms to counter their foe; these will inherently include some guesswork and miscalculation. But the larger objective of these processes may be to support the command and control of military forces, offering an unwelcome vector of opportunity for emergence from the ultra-tactical realm to drive anticipated behavior in the tradition tactical environment.

Moffat [10] identifies six key properties of complexity important to networked command systems used in warfare. *Nonlinear interaction* can lead to "surprising and non-intuitive behavior;" *decentralized control* can facilitate emergent behavior generated through local coevolution; *self-organization* can occur without external guidance; *nonequilibrium order* means there is never a steady-state; *adaptation* involves clusters or avalanches of local interaction that are constantly being created or dissolved; *collectivist dynamics* reflect the ability of elements to influence each other and cause ripples effects throughout the system. These properities are consistent in principle with the system dynamics and behavior that produce Black Swans and Dragon-Kings.

Another approach [11] is to examine modern military command and control through the lens of the Perrow safety engineering model using two main parameters—the interaction of parts (linear or complex) and the coupling characteristics (tight or loose). Of the four basic combinations of these parameters, systems that are tightly coupled with complex interactions (i.e., those in the realm of Dragon-Kings) are the highest risk. This is due in part to the conflicting operating requirements—that is, control of complex interactions is best decentralized; control of tightly coupled processes are best centralized. So, designing a centralized command and control system for automated cyberspace operations (defensive or offensive) is a high risk venture from both the perspectives of complexity modeling and safety engineering.

C. ULTRA-TACTICAL OPERATIONS GONE AWRY

To better understand these concerns regarding such behavior in cyberspace, consider the 2010 flash crash of U.S. futures and securities markets [12]. On May 6, 2010, major equity indices in both U.S. futures and securities markets suddenly plummeted 5 to 6 percent in a matter of minutes. During this time, over 20,000 trades across more than 300 securities were executed at prices more than 60 percent away from their values just moments before. Many of these trades were executed at prices of a penny or less, or as high as $100,000 – ranges that would not have been approved by rationale humans. Most of these trades were cancelled via formal intervention after the market closed.

One could assert that such trading operations have evolved far beyond the original intent of a stock market to connect investors with capital to prospective revenue-generating venues. Instead, it has largely moved toward making large volumes of purchases and sales to leverage microscopic changes in the perceived value – often with little regard for the long-term prospects of the stock (or market writ large). Osorio and others [13] observed that as early as 2001, the distribution of high-frequency stock market events included autocorrelations in volatilities and volumes caused in part by a herding attitude amongst traders. These effects were magnified as trading became faster and more automated. By May 2010, market dynamics were dominated by automated responses implemented with the willing abdication of the cognitive. Automated algorithms--individually well designed--interacted in such a way as to produce a Dragon-King that dropped market value dramatically. Although the U.S. Government report outlines many contributing factors to this event, no one has been able to determine exactly how it occurred or how to prevent future occurrences. A reasonable conjecture is that the internal models of the algorithms were tacit ones concerned only with immediate profit opportunities with little overt elements to examine alternatives or consider the overall system stability.

Further examination [14] of the ultra-tactical transactions surrounding the “flash crash” uncovered over 18,000 ‘ultra-fast” Black Swan events—either mini-spikes or mini-crashes—that had millisecond-scale durations. In this light, perhaps the proper cybersecurity perspective to adopt is one less worried about a “cyber Pearl Harbor” and more concerned about a “cyber tsunami” or “cyber Super Storm Sandy.”

4. CONTEXTS OF HUMAN COGNITION

Recall that the concept of the ultra-tactical is that of an additional realm of operations in the traditional strategic-operational-tactical framework and that

its discrete processes occur well below the level of human cognitive processes. However, the ultra-tactical processes and their aggregate results may be used to aid human decision making in traditional operational spectrum where human cognition dominates.

A. ENHANCED DECISION MAKING

Figure 3 depicts a full operational spectrum from strategic down to ultra-tactical time scales. At the strategic level, deterrence is practiced based on existing policy; at the operational level, deliberate responses to cyberspace activity reflect doctrine and planning; and at the tactical level, more immediate deliberate responses are based on tactics, techniques, and procedures. In the ultra-tactical realm, automated responses are based on a priori design. Anticipating that these designs will be standardized and coupled, it may also create a breeding ground for Dragon-Kings as well as a quandary for implementing either centralized or decentralized control of the processes.

But, within this spectrum, where and when should human cognition be engaged to enhance the overall process? Risky emergent behavior is possible at any level, but the time scale to address any emergence increases in the ideal case; that is, strategic issues may have a greater luxury of time for examination and policy may be broad to allow flexibility in application. When implementing automated responses we have willingly abdicated the option of cognitive processes based on what we think may occur. In doing so, we must ensure these responses can differentiate adversarial threats from natural emergent behavior and that they are robust enough to accommodate the dynamic nature of cyberspace.

Tyugu [15] examines the use of command and control agents in cyber warfare, noting the trend toward increasing use of automatically operating entities, with one critical factor being the speed of automatic decision making. Regarding the command and control of intelligent agents (i.e., ones that have some independence) he notes that their behavior is harder to predict due to possible misinterpretations of the situation, the command, and priorities. These agents may operate autonomously oriented toward a goal using a beliefs-desires-intentions framework, perhaps following a tacit internal model focused on a desired state vice examining alternatives. This situation may be exacerbated in multi-agent systems, with a specific threat being the "formation of unwanted coalitions by agents," an outcome consistent with the adaptation and collective dynamics of Moffatt. Klein and others [16] have explored initial frameworks to react to detected attacks (such as denial of service) using automatic responses, hoping to improve speed and reliability.

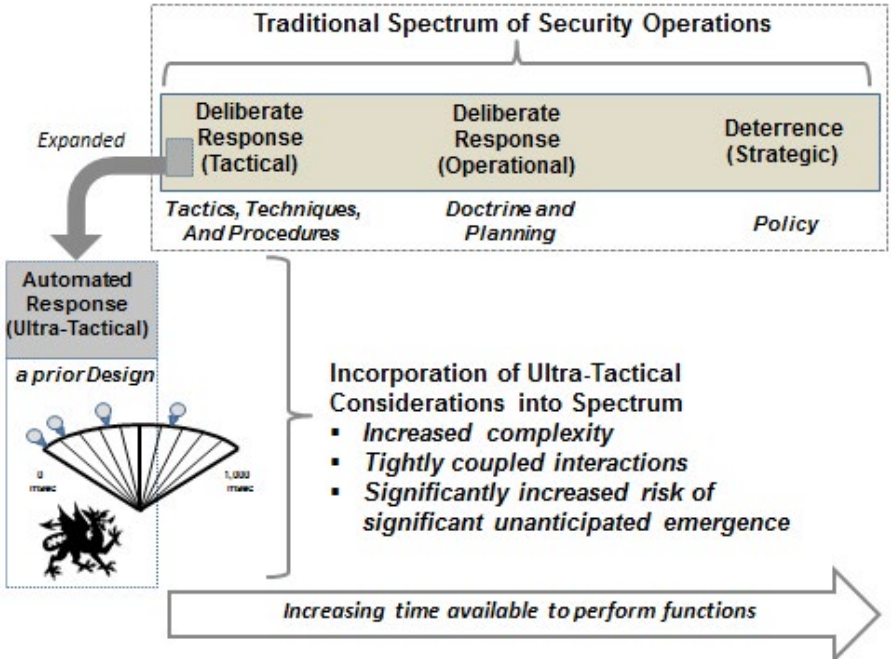

Figure 3. Operational spectrum with expanded ultra-tactical events

Accomplishing this requires information from a diversity of resources passed along many paths—definitely a useful opportunity to apply ultra-tactical processes, but the design should also guard against emergence in the response options that are generated.

B. POTENTIAL BIASES

A crucial part of building confidence in the design of ultra-tactical processes is to fully consider and mitigate the consequences of unchecked cognitive biases in their design. To add further challenge, cognitive bias encountered during design or operation introduces the dilemma of actual versus perceived reality. For example, aural and optical illusions exploit shortfalls in cognitive processes, sometimes to the degree that you cannot force your perception to recognize the reality once the illusion is revealed. For example, the McGurk effect demonstrates how human perceive different sounds from identical sounds under different visual references of human mouth movements [17]. Such mechanisms are more than mere parlor tricks; fully understanding these phenomena is crucial to achieving objective and insightful situational awareness during both the design and operation of cyberspace systems.

Since all the activities in the spectrum are developed a priori to some degree, they are all sensitive to changes in the dynamic cyberspace environment. MacNulty [18] has examined how values, cultures, and beliefs relate to mental models and perceptions across the spectrum of conflict. Because of different value systems, individuals and groups may not perceive the world in the same way and therefore may not respond to communications, hardships, and crises as predicted. Tyugu [19] notes that many human factors influence the development of command and control models. These factors (such as intent, rules & constraints, roles & responsibilities, and situational assessment) could introduce significant biases into the development of automated agents operating in the ultra-tactical realm. Geers [20] included as his ninth aspect of the future cyber battlefield that "the intangible nature of cyberspace can make the calculation of victory, defeat, and battle damage a highly subjective undertaking." Indeed, it will remain a challenge to define the beliefs-desires-intentions parameters for intelligent agents that will operate effectively and appropriately in both the desired future environments as well as potential alternative futures. Realizing that there is no way to predict the complex future, how can one evaluate ultra-tactical processes in future situations?

5. FUTURING METHODOLGIES

Futuring methodologies can develop feasible operational scenarios for use in evaluating the benefits and risks inherent in implementing automated responses that operate without human cognitive interaction. Clearly, there exist many probable futures to consider for the given spectrum of cyberspace activities. These futures will have various degrees of dynamic activity, but at the ultra-tactical scale, all will deal with a cyberspace environment that is constantly changing. Thus, merely applying a tacit model of linear or even exponential extrapolation to define a discrete future has limited applicability. Instead, it is useful to develop an envisioned future scenario without the constraints of having to plot a logical path to its existence (a potentially fruitless situation given the nature of complexity and emergence).

A useful tool for assessing future events is to develop sets of future scenarios that encompass areas defined by divergent conceptual axes. Ogilvy and Schwartz [21] offer a simple and effective model for developing sets of scenarios that use deductive logic to build outcome plots—based on two dimensions of uncertainty--that can capture the scope of many possible outcomes. They recommend having diversity in teams that develop scenarios to help reduce individual biases. Of course, implementation requires the commitment of resources and preferably external facilitators.

Figure 4 depicts an example to illustrate the process of constructing a futuring

scenario diagram. The first dimension of uncertainty (the diagram x-axis) addresses the use of automated defenses in cyberspace--at one extreme is use limited to only the military, the opposing end is global use. The second dimension of uncertainty (the diagram y-axis) is the degree to which military cyberspace operations use the Internet—at one extreme is stand-only operations separate from the Internet, the opposing end is operations fully integrated into the Internet.

The axes of the plot form quadrants offering potential situations for detailed scenario development as does the center of the plot in most cases. It is useful to name the quadrants using simple titles that quickly convey the essence of the situation. In our example, the center scenario is called "Status Quo" and could be developed as an extrapolation of the current situation of the presence cyberspace automated defenses in both military and global applications and the partial use of the Internet by military systems. The upper left quadrant is called "Spill Over" since it indicates a situation where only the military has automated defenses with the possibility that the effects of the automation could spill over into the Internet. The upper right quadrant, "Mixed Signals," signifies how the global use of automated defenses and full integration into the Internet makes it difficult to differentiate the effects caused by military operations from those occurring from other sources.

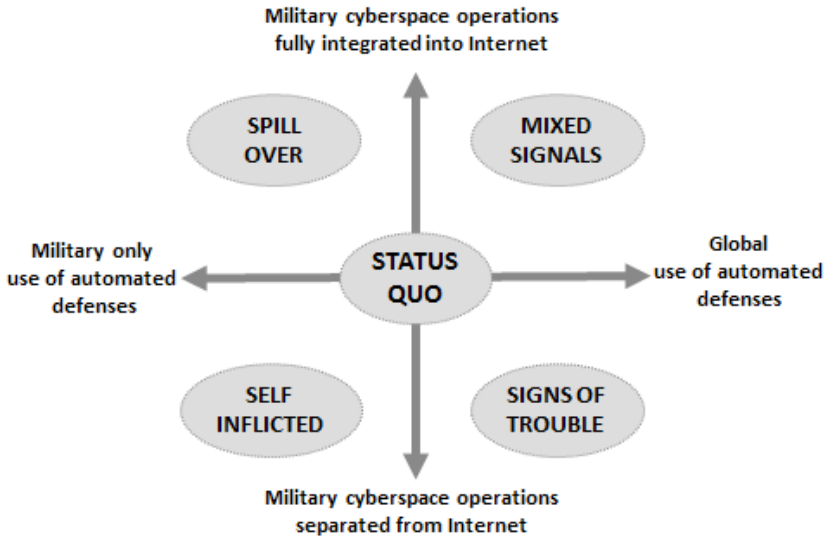

Figure 4. Example futuring scenarios

Since it represents an environment of a diverse community of moderately coupled systems, it would be a likely source for Black Swan events. The lower right quadrant is

called “Signs of Trouble” since the military could observe problems with automated defenses in the global Internet environment, but not be directly affected because its systems are separate from Internet. Finally, the lower left quadrant, “Self Inflicted,” represents the case where only the military uses automated defenses and that these are limited to stand alone systems, thus any problems must be internally generated. Because this quadrant is an environment of largely homogeneous systems that are tightly coupled, it is likely to spawn Dragon-King events.

Once the initial framework of the scenarios is complete, details can be added to better describe the possible future. Each scenario can then be explored to identify possible issues, challenges, and opportunities as well as how they may be addressed, mitigated, or exploited. The more detailed scenarios can then be compared to identify common themes as measures or actions that work effectively in multiple scenarios; these are good candidates for resilient design consideration. This process can be repeated using different dimensions of uncertainty to generate new scenarios. Clearly this is an iterative process that can be accomplished in a collaborative workshop venue. Remember that development, examination, and comparison of the scenarios help provide extensive and robust insight into what *may* happen, not a discrete and limited prediction of what *will* happen. Emergent events (e.g., Black Swans and Dragon-Kings) may also be examined using “Wild Card” scenario methods [22]. The presence of such emergent events can impact the situational awareness of decision makers in the scenarios. For example, Tyugu [23] extended his concerns regarding multiple agent operations into a “Scary Scenario” where very intelligent cyberspace agents may follow intentions and priorities of their own—potentially drawing response from other defensive agents. Such a future emergent event could be viewed as a Dragon-King resulting from complex interactions originally designed for goals quite different from those that emerge, all forming and evolving at potentially ultra-tactical speeds.

A broader value of developing scenarios of alternative futures is their use to assess the vision, mission, and goals for the organization’s desired future [24]. The comparison of these futures may provide insight to weaknesses in the current strategies that can be adjusted to provide a more robust and resilient future strategy. Healy [25] developed five scenarios to examine the future of conflict and cooperation in cyberspace. This included an assessment of the stability and likelihood of these futures occurring. These scenarios could serve as possible starting points for brainstorming dimensions of uncertainty to construct future ultra-tactical vignettes.

6. SUMMARY

Military cyberspace operations—offensive and defensive—envisioned for the near future may make extensive use of automated response processes that occur well below the threshold of human cognition. This realm can be modelled as an ultra-tactical portion that expands from the traditional tactical-operational-strategic spectrum. Complex interactions in this realm will lead to unanticipated emergent behaviour with potentially significant negative effects on planned operations. Current agents designed to operate automatically may be limited to tacit internal models that focus on a desired future outcome and may not consider the alternative futures to reduce risk. Their design may also reflect unchecked biases embodied in the beliefs-desires-intentions objectives of their desired outcome. Futuring scenarios can facilitate the examination of a wide range of possible alternative outcomes that can be incorporated into the development of more robust and resilient processes in the ultra-tactical realm.

REFERENCES

[1] L. Panetta. Remarks on Cybersecurity to the Business Executives for National Security, New York, 11 October 2012.

[2] K. Alexander. Statement before the House Committee on Armed Services, Washington, D.C., 20 March 2012.

[3] K. Alexander. Statement before the Senate Committee on Armed Services, Washington, D.C., 12 March 2013.

[4] J. Caton. "Beyond Domains, Beyond Commons: Context and Theory of Conflict in Cyberspace," presented at the 4th International Conference on Cyber Conflict, Tallinn, Estonia, 2012.

[5] K. Geers. Strategic Cyber Security. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012, pp. 103, 109.

[6] T. Czerwinski. *Coping with the Bounds: Speculation on Nonlinearity in Military Affairs*. Washington, D.C.: National Defense University, 1998, pp.7-27.

[7] D. Sornetter. "Dragon-Kings, Black Swans and the Prediction of Crises." Int. J. of Terraspace Sci. and Eng., pp. 1-18, 2009.

[8] D. Geer et.al. "Cyber*In*security: The Cost of Monopoly. How the Dominance of Microsoft's Products Poses a Risk to Security." Computer and Communications Industry Association, Washington, D.C., 24 September 2003.

[9] K. Geers. Strategic Cyber Security. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012, pp. 41.

[10] J. Moffat. Complexity Theory and Network Centric Warfare. Washington, D.C.: DoD Command and Control Research Program, 2003, pp. 42-43.

[11] T. Czerwinski. "Command and Control at the Crossroads," *Parameters*, vol. XXVI, pp. 121-132, Autumn 1996.

[12] "Finding Regarding the Market Events of May 6, 2010: Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues." Washington, DC: U.S. Commodity Futures Trading Commission and U.S. Securities and Exchange Commission, Sep. 30, 2010.

[13] R. Osorio, L. Borland, and C. Tsallis. "Distributions of High-Frequency Stock Market Observables" in *Nonextensive Entropy: Interdisciplinary Applications*. Edited by M. Gell-Mann and C. Tsallis. New York: Oxford University Press, 2004, pp. 321-334.

[14] N. Johnson et al. "Financial black swans driven by ultrafast machine ecology." technical working paper, Cornell University Library, Ithaca, NY, Feb. 2012.

[15] E. Tyugu. "Command and Control of Cyber Weapons," in *Proc. 4th International Conference on Cyber Conflict*, 2012, pp. 335-341.

[16] G. Klein et al. "Enhancing Graph-based Automated DoS Attack Response." *Proc. 2009 Conf. on Cyber Warfare, NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia, 2009.

[17] L. Brancazio and J. Miller. "Use of visual information in speech perception: Evidence for a visual rate effect both with and without a McGurk effect." *Perception & Psychophysics*. 67(5), pp. 759-769, 2005.

[18] C. MacNulty. "Values, Resiliency & Strategy in Cyberspace." presented at Army War College Cyber Futures Workshop, Carlisle Pennsylvania, 13 December 2011.

[19] E. Tyugu. "Command and Control of Cyber Weapons," *Proc. 4th International Conference on Cyber Conflict*, 2012, pp. 335.

[20] K. Geers. Strategic Cyber Security. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012, pp. 109.

[21] J. Ogilvy and P. Schwartz. "Plotting Your Scenarios." Emeryville, California: global Business Network, 2004.

[22] J. Dewar. "The Importance of 'Wild Card' Scenarios." Santa Monica, California: RAND, 2009.

[23] E. Tyugu. "Command and Control of Cyber Weapons," *Proc. 4th International Conference on Cyber Conflict*, 2012, pp. 340-341.

[24] "The Future Belongs to Those Who…A Guide for Thinking About the Future." Alexandria, Virginia: Institute for Alternative Futures, 2009.

[25] J. Healy. *The Five Futures of Cyber Conflict and Cooperation*. Washington, D.C.: The Atlantic Council, 2011.