MINERVA
RESEARCH
INITIATIVE

FY19 MINERVA TOPICS OF INTEREST

Below represents the Minerva topics of interested for FY19. We anticipate an open Funding Opportunity Announcement related to these topics in the near future. Further information will be forthcoming, when available.

Topic 1: Peer/Near-peer Statecraft, Influence, and Regional Balance of Power
Topic 2: Power, Deterrence, and Escalation Management
Topic 3: Alliances and Burden Sharing
Topic 4: Economic Interdependence and Security
Topic 5: Economic Viability, Resilience, and Sustainability of Logistics Infrastructure
Topic 6: Multi-Domain Behavioral Complexity and Computational Social Modeling
Topic 7: Autonomy, Artificial Intelligence, Machine Ethics, and Social Interactions
Topic 8: Models and Methods for Understanding Covert Online Influence
Topic 9: Automated Cyber Vulnerability Analysis

Topic 1: Peer/Near-peer Statecraft, Influence, and Regional Balance of Power

In line with the 2018 National Defense Strategy, this topic is especially interested in the role of great powers within the international system; in the interactions of peer and near-peer state actors and how to methodologically and analytically research the sociopolitical context of statecraft and influence. It will prioritize proposals that offer innovative, interdisciplinary insights into thematic topics including:

- The role of great-powers in managing global stability: How are traditional and emerging great-powers'—including but not limited to China and Russia—understandings of security impacted by the social, cultural, commercial, economic, and political environments in which they exist and what factors shape the ability of great-powers to mobilize within and beyond their territories? To what extent do culture and society determine how the identities of great powers evolve and how do those identities shape their perceptions of security and interactions with other states? How does the political influence on commercial and economic activities create a landscape of statecraft opportunities? How do structural changes among various states affect global order and create a "new global order"? Do changing ideological visions impact the utility of multilateral alliances? How do non-state actors influence established state mechanisms for managing conflict?
- The concept of the balance of power in ordering and shaping great power relations within contemporary and historical international systems, including how great powers understand their status in relation to one another and efforts to transform their momentary favorable position into an enduring strategic advantage. Here, the question is how states seek to shape or achieve a favorable balance of power and the range of military, diplomatic, and economic instruments they employ for this purpose. Key questions of interest include: How do we study the role foreign influence, foreign investment, emerging technologies, and military exports play in the balance of power? What elements comprise a balance of power and how do these relate to understandings of international order? How do states achieve a (favorable) balance of power and what is the role of

the military in relation to other tools of state? How have balances of power varied historically or across different parts of the world? How do balances of power emerge in regions where they were previously absent? What is the relationship between regional and global balances of power?

- Influence underlies effective statecraft and power alliances, but nuances of what constitutes a productive strategy of influence is situationally dynamic and complex, occurring across multiple domains of competition and cooperation. As such, there is interest in understanding what contributes to favorable influence (including and beyond soft power) with allies and adversaries? What factors affect state decisions in effort to influence other states and regional bodies? Work should include approaches for validating causal dynamics between specific influence strategies and outcomes as well as the advancing of theory that allows a prediction of outcomes resulting from influence. Alongside this, understanding how multi-domain competition works in relation to influence will be important. How do nations compete selectively when in a disadvantaged environment? What governs the calculative dynamics of various competitors' behavior? How do peers and near-peers compete for influence in ungoverned and semi-governed spaces, especially dominance in space and cyber domains? What role does emerging technology and technological dominance play in asserting influence?

Topic 2: Power, Deterrence, and Escalation Management

This topic supports basic research on power, influence, and escalation management methodologies with an emphasis on empirically tested or theoretically founded decision support tools for selecting the best strategies. A continued emphasis on multidisciplinary approaches to generate new theories and methodologies that incorporate strategy and strategic thought, psychology and decision-making, area studies, and culture, sociology and economics are needed to understand the potential and limitations of power, influence, and escalation management options and to understand how to develop predictive capabilities. Additionally, an emerging area of interest is "deception" by nation states, particularly through use of media, traditional and social as well as the use of cyber instruments as a non-traditional means of power projection and influence, and economic pressure through stimulus packages with unruly consequences to non-payment of loans.

The information environment includes multiple platforms, social communities, and topic areas that are polluted with disinformation and attempts to manipulate state decision and population beliefs and decisions. Currently there are not well-formed theories on how these campaigns are used, how their efficacy is measured, and how they fit into larger power, influence, and/or escalation management campaigns.

Emerging powers—including Russia, China, and Iran—have an increasing presence in black market environments, though little is understood about the structures and strategies that occur in these contexts. Also, we lack scientific understanding of the impact of black-market strategies on U.S. operations and interests, despite the proliferation of these markets. Another area of interest is the use of cyber tools in support of nation states more traditional power and influence strategies.

This topic seeks predictive models of power, influence, and/or escalation management strategies in shaping the future of broad regions as well as specific hot-spots and whether generalized theories allow lessons learned in one region or hot spot to be applied to another region. Theories that establish causality between action and outcome and action and prediction are desired on power projection, influence, and escalation management strategies to predict and measure their ability to shape an area of interest. The aim is to make it easier for US and allies to identify the best strategy for a situation and to recognize strategies that are most dangerous options for the US and allies. Specific areas of interest include the use of power projection/influence/escalation management actions on/between peer states, non-state institutions, rising military powers and rogue states.

Power projection

- Drivers affecting how a state or states influence other states.
- For those drivers, what observables (direct and/or proxy) can determine if actions are effective?
- Novel approaches for validating the causal dynamics between specific *power projection strategies (diplomacy, information, military, and economic* (DIME)) actions and outcomes
- Advancing theory that allows a prediction of outcomes resulting from power used by A on B.
- The balance of power between the state and other traditional and non-traditional institutions
- The use of cyber and black markets to project power.

Deterrence Theory

- Drivers affecting how states decide how to deter decisions made by others
- For deterrence drivers, what observables can be used to determine if actions taking are effective?
- Measuring the balance of power between the state and traditional and non-traditional institutions
- Approaches for validating causal dynamics between specific deterrence strategies and outcomes.
- Advancing theory that allows a prediction of outcomes resulting from a deterrence

Beyond conventional deterrence and power projection

- Approaches for the intentional use of deception to influence
- For deception, what observables can be used to detect its use and to determine if actions are effective.
- Approaches for validating the relative importance of deception on outcomes
- Advancing theory that predicts outcomes resulting from the use of deceptive actions

Shaping theory:

- Approaches for using military strategic action to influence future actions by other states
- What variables can be used to detect its use and to methods to measure its success
- Approaches for validating the relative importance of military

Escalation management

- Approaches for validating the relative importance of power/influence actions on outcomes
- Advancing theory that predicts outcomes resulting from multiple power and influence actions
- Theory governing the use of power and influence concurrently
- Frameworks for escalation dynamics in reciprocal power and influence actions

Area studies

- Social, cultural, economic, and historical factors affecting success/failure of power projection or influence actions applied to an area to shape decision spaces, and application to the realities of today
- Social, cultural, and historical factors affecting the choice of power projection or influence actions to shape the decision space of others, and application to the realities of today.

Operational effectiveness

- What combination of power/influence/escalation management techniques, under what conditions are successful in creating decision outcomes that favor US and Allied interests? Given successful decision outcomes, can those techniques be generalized and applied to similar or varied conditions?

Topic 3: Alliances and Burden-Sharing

Global security in the contemporary world is characterized by inter-state alliances. The dynamics of these alliances may vary substantially, depending on the partners to alliances, the resources they bring to the alliance, and the objectives of the different allies. One challenge is ensuring that the different partners contribute to common objectives. Allies, however, may have different resources to bring to the table, different objectives with respect to maintaining an alliance, and different perspectives on what constitutes a fair distribution of the burden for maintaining an alliance. That is, burden-sharing is a complex issue that depends on the interests of different partners, their resources, their goals, and the extent to which their goals are being met. An ever-present risk in forming an alliance is that one's partner(s) will free-ride. That is, one or more agents may take advantage of the resources others bring and access those resources for their own interests without providing comparable contributions to the alliance.

Scientific research in this problem domain of burden-sharing in alliances is scant, although social science has a long history of research on social exchange, distributive justice, social network analytics, and economics, all of which may be relevant to addressing this issue. These and other scientific approaches require scaling to more macro scales to address the issue of global alliances and burden sharing. Additionally, cultural variation, international agreements, national policies/laws, regional economies, and governance structures may all play a role in shaping the form of burden-sharing and capacity to limit free-riding. This Minerva topic seeks to support research that will generate and validate new models to better capture the dynamics of burden-sharing in alliances with attention to factors that limit or eliminate free-riding. Empirical questions that the research should address may include:

- What are the incentives for burden-sharing within alliances?
- What constraints limit burden-sharing in alliances?
- How does burden-sharing differ within the context of bilateral and multilateral alliances?
- How do changes in the alliance partners impact burden-sharing?
- How can states more effectively manage alliances in order to achieve a greater degree of burden-sharing?
- How do we measure the depth of a relationship as opposed to the perceived depth of a relationship in relation to the return of investment on the relationship? What types of actions undermine the strength of alliance relations and what areas increase confidence in the relationship?

Topic 4: Economic Interdependence and Security

Great power competition is taking place in an international system characterized by high levels of economic interdependencies. These interdependencies may have implications for how states pursue their national security and defense objectives. Yet there is little basic scientific understanding of how these economic relationships arise and evolve. Moreover, the short- and long-term implications of these relationships have not been accurately modeled to provide insight on how economic interdependencies impact a state's national security and defense objectives. The interdependencies are often multi-faceted (e.g., involving a complex network of trade partners that changes over time and involves different goods/services exchanges). Depending on the market, balances of power in the economic sphere may change suddenly and rapidly, or may be relatively stable over time. The factors that impact such balances may include governance shifts, cultural change, technological innovations, educational opportunities, entry/exit of trading partners from a market, and other factors that have consequences for the network of states engaged in economic relationships.

This Minerva topic seeks to develop new approaches to studying complex economic interdependencies and assess the implications of those interdependencies for national security among the nation states in the networks. Ideally, data and models will capture longitudinal relationships and identify how those relationships change over time, are linked to policy, relationships, and operational outcomes relevant to the states in the networks. Questions of interest for this topic could include:

- What is the relationship between economic solvency and national security?
- What are the implications of economic interdependence for states in diplomatic and military competition with each other?

- How do states use their economic power to achieve national interests in competition short of armed conflict?
- To what extent have economic instruments been used as effective means of coercion in international politics?
- How do different states understand the nature of a free-and-open market and fair competition? What do these difference conceptions mean for how large economies wield their economic influence? Where do OECD countries agree and disagree?
- What are the different models for understanding and managing anti-trust or non-competitive commercial behavior? Where do these models agree or disagree? Where are these models prominent?

Topic 5: Economic Viability, Resilience, and Sustainability of Logistics Infrastructure

Logistics centers, whether they are ports, airports, road, or rail hubs, are critical to a country's global and sub-national trade. They are the major nodes for commodity imports and exports, and thus are critical infrastructure. They need to be (re)built or expanded in the aftermath of armed conflict, and they remain vulnerable to disruption from further civil strife, terrorism, natural disasters, and climate change.

Logistics centers may serve large hinterlands. Specific sites may be a country's primary portal for commodities not produced in country. In many cases, these are critical products—food, medicines, etc. Developing countries are often dependent on natural resource exports—e.g. oil, timber, textiles—that are competitive only via centralized transport (often, most economically, via ocean). In conflict zones, ports and airports often incur damage and their major connections inland—railroads and highways—are destroyed or deteriorated. Government institutions required to manage trade may no longer function. These damages reduce capacity and lead to large economic losses. Terrorism, natural disasters, and sea level rise associated with global climate change often exacerbate these losses. Logistics centers can thus become chokepoints for the continuation of commerce and economic development in the aftermath of conflict. Natural aftermath of these events opens opportunity for replacement of manual systems for cargo and natural resource movement with automated systems for increased economic prosperity and increased vulnerabilities to statecraft manipulation.

This research topic focuses on the role performed by logistics centers as critical infrastructure for societies to be economically viable, resilient, and sustainable in the aftermath of conflict. Sub-topics of interest include:

- A systems analysis of logistics centers and interior regions in terms of infrastructure (re)construction and expansion, economic interdependence, logistical operations, vulnerability, and resilience analysis. This helps inform the strategic importance of ports, airports, and rail hubs in conflict zones and regions of economic expansion.
- More nuanced analysis of critical logistics and infrastructure configurations, including surface transportation. This also integrates workforce training of management and front-line employees.
- Vulnerability analysis in terms of probabilistic assessments of threats and the direct and indirect intraregional consequences of disruptions to critical logistics centers.
- Resilience analysis regarding strategies and tactics to regain functionality and optimize the time path of repair and recovery.
- Computable general equilibrium modeling of economic interdependence, vulnerability, and resilience. Prior analyses have utilized ad hoc methods that only partially resolve the path-dependence issues of resilience analysis.
- Dynamic optimization of the large investments logistics centers/infrastructure represent and their connection networks require, and the long life span of these investments.

- How can we evaluate the interdependence between economic viability and information dependence? Does control over networks yield systemic advantage to the commercial firms of other competitors? Can states create commercial advantages for their firms by influencing standards?

Topic 6: Multi-Doman Behavioral Complexity and Computational Social Modeling

Warfare is a complex, large-scale enterprise, subject to many uncertainties, difficult to control, and yet which must be predicted as accurately as possible. The globalization of trade, technological infrastructures, and access to natural resources has resulted in complex and often hidden dependencies in the economic and technological networks, bringing significant uncertainties in the value of the outcome, as well as in the optimal strategy of such a conflict. From a game-theoretic point of view, we must deal with a multi-player hierarchy in a very large parameter space, and with uncertain and time-varying objectives.

This research topic addresses the imperative to understand better both the short-term and long-term consequences of all types of actions associated with total warfare in a complex, multi-domain framework. It covers how total warfare could be conducted and aims to discover connections leading to the failure of executing strategic and tactical planned military actions, or their degradation. Conversely, it also aims to identify strategies that would safeguard these plans against such cross-domain disruptions. This will require research on several fronts, which must be ultimately integrated into a comprehensive capability which would adequately describe the complexity of the problem, model the dynamics (i.e. the state evolution), and infer optimal strategies. The main aspects of interest are:

Cross-Domain Relationships in Total Warfare

While regional conflicts have been the norm in recent years, the focus of attention is shifting to scenarios involving larger-scale engagements, with peer or near-peer competitors. This is especially relevant as some actors are actively pursuing a strategy of "total warfare", where every domain becomes a battlefield, be it cyber, economic infrastructure, social media, environment, etc., as well as the traditional military domains and capabilities.

Research is required to support identification and fundamental understanding of inter-relationships between different domains of influence, e.g. social, economic, political or legal, that is both *representative* and *predictive*. Here, *representation* means that one should be able to accurately describe the state of the domain. In particular, one should also be able to evaluate the sensitivity to the various domains and the possible actors. The *prediction* aspect implies that the interactions between the domains and their elements can be cast into a form that can be fast-forwarded in time, whether by interpolation, mappings, or time-stepping algorithms.

This requires a very careful and rigorous analysis of events, the social and economic conditions, and sound reasoning. It is also a multi-disciplinary task. Besides sociological and economic expertise, the ability to manipulate potentially large amounts of data and extract information from various sources may also prove to be critical. We can gain insight from historical analysis, whether small or large-scale events, and specifically seek the (initially) subtle effects of correlated events in non-military domains, that have military and strategic implications. In addition, a focus on more remote events and decisions, which may appear unrelated at first, may offer insights into a cascading effect across the social and economic layers and impact military campaigns, even at later times. By reaching deep into this causal network, one can gain a better sense of the scope of the complexity, and inform future models.

Societal Resilience in Cross-Domain Warfare

Total warfare across multiple domains is likely to challenge societal resilience, particularly in the event of any protracted conflict. The effects of conflicts upon society is likely to extend beyond the immediate kinetic impacts to encompass the social, political, and economic institutions and relationships that underpin societal cohesion. Better understanding of the nature of the interrelationships across domains will yield insights into the effects of protracted warfare on societies, particularly in an era of technological developments that blur the lines between civilian and military spheres. Researchers are encouraged to consider how to evaluate societal resilience of all actors involved, and how that may evolve over extended timeframes.

This topic is interested in research and strategies that would support planning against cross-domain disruptions. This is a more difficult problem; the adversary could experiment with any action(s) that would sow chaos, until finding one with a maximal impact, while designed protection against such attempts would require examining all possible actions. A practical outcome here is the identification of trends and general rules, which may not provide strict guarantees, but useful guidance for reducing the scope of the search for threats and make the problem solvable. In turn, this provides information about which policies to formulate and implement, that would minimize the socio-economic damage while also minimizing the resources required for their implementation.

AI in Cross-Domain Total Warfare

An important evolutionary trend concerns the increasing reliance on artificial intelligence (AI) at multiple levels of sophistication. The consequences of this explosive growth of AI in the entire socio-economic and military ecosystem, and the implications on national security, are not well understood. Threat analysis which relies on the understanding of group behavior may no longer apply; machine intelligence is not subject to emotional drivers and does not respond to mechanisms of social influence. If the intelligent machines are designed and trained with objectives and rules that originate from a few human actors, they effectively become replicas with little or no variation in behavior; statistical averaging becomes meaningless, and this increases the brittleness of the whole ecosystem. The AI becomes a new class of "alien" actor which does not obey the same rules, and yet it is turning into a dominant factor in the evolution of *all* the socio-economic and military networks. There is no comprehensive theory on how to characterize, understand, and model this blended human-AI sociology. Exploratory advances in this area are also desired.

Computational Modeling of Large-Scale, Cross-Domain Behavioral Dynamics

Computational science applied to socio-economics provides a powerful remedy, *if* accurate models for elementary interactions can be effectively implemented, and if the problem complexity can be scaled to within practical limits. Although various approaches can be considered and/or mixed, agent-based modeling (ABM) is a traditional yet powerful approach that can offer specific insights. We can then consider an ABM-network for each domain; financial (e.g. banks), industrial (factories, refineries, etc.), transportation (airlines, trucking, trains, etc.), etc. Agents can be linked to multiple networks, allowing cross-domain influence and the propagation of critical events (failures, jamming, paralysis, etc.). By predicting the range of actions and consequences of networked agents, one can aim at being able to reproduce total warfare scenarios *in-silico,* in a realistic and practical fashion.

To make computational models tractable and fully unleash their predictive power, we must be able to make progress along several directions. First, one must be able to reduce the complexity of the real world in a systematic and rigorous fashion. The higher the complexity of the representation, the higher the computational cost in evaluating "distances" or in performing additive, combinatorial, or averaging operations. Thus, this topic calls for advances in the design of representative (multi-dimensional) variables for complex description of agent states and motivations, as well as in the mathematical and numerical methods that model the socio-dynamics between the agents and these state variables.

A second problem is the development of methods to track the dynamics and the correlations of actions between the various domains. We need to be able to simulate a “perfect storm” in the context of multi-domain, total warfare, and examine resiliency of the networks. Practically speaking, the dynamics of the agent-based ecosystem cannot be analyzed a-posteriori, for arbitrary time delays; this suggests that iterative procedures should be used, and/or the causality chains should be “learned” via a repetitive exploration of scenarios. Such approaches have the potential to dramatically focus on the most important chains of events, considerably reducing the dimensionality of the parameter space, and would dramatically expand our predictive abilities in very complex scenarios. These problems are challenging for both their sociological and mathematical aspects, and call for tightly coupled multi-disciplinary solutions, leveraging advances in multiple fields.

Topic 7: Autonomy, Artificial Intelligence, Machine Ethics, and Social Interactions

The emergence of Artificial Intelligence (AI) presents opportunities for machines to augment human decisions and actions and it is certain to have sweeping social impacts, changing many aspects of how we live, learn, and communicate. The vast majority of research in this domain has focused on how AI can augment human performance, yet the use of advanced machine intelligence in complex situations characterized by moral dilemmas creates a precarious challenge for human tolerance/acceptance of machine actions. How do humans interact with machines when they take actions (or make decisions) that have negative consequences for humans? This challenge goes beyond the current liability issues facing the automotive industry, and extends to human perceptions of machine action. Fundamental research is needed to identify and isolate the psychological factors that influence human acceptance of machine actions in contexts where these actions can cause negative consequences to humans. Further, research is needed that understands both the ethical implications of AI social interactions as well as the environment of operating ethically in relation to an adversary or a coalition partner who may have a very different understanding of the limits of machine behavior. Relevant questions here include: How do relationships develop with machines, especially relationships of bidirectional trust? How does a reliance on machine intelligence affect human relations within communities, societies, and global order more broadly? How do social and moral norms shape the apportion of autonomy? How does reliance on autonomy shape individual and organizational decisions? For example, in human organizations, delegating serves to increase the moral distance from the consequences of one's actions. Might operating combat through robotic controls decrease empathy and increase dehumanization of others?

A related interest of this topic is analysis that interprets the dynamics of human and human-machine interaction, the synchrony or desynchrony of speech, posture, movement, reaction timing, emotional expression, and ownership of intellectual property. Any effort in behavioral informatics must be broad and multimodal. The common approach to computerized image understanding will not suffice. It is important to distinguish proposed work from research already underway or already accomplished. The social science context of the research must be articulated around AI and sociality, and it must offer predictive utility, not just retrospective analysis.

This topic invites novel approaches to understanding the implications of social interactions with machines and how such interactions may vary across cultural environments, especially those of peer and near-peer states. Are there cross-cultural universals in interacting with autonomy or are there culture-specific nuances that lead to different expectancies for automated behavior? Broad questions about trust, mentioned above, should construe trust as a bidirectional relation, involving both the human and the machine’s ability to interpret a partner’s goals, moral concerns, tacit assumptions, and framework of expectations and commitments. Research along these lines will be increasingly important as AI systems develop more sophisticated, dynamic, and unscripted partnerships with humans.

A project along these lines must offer an approach to discovery. It should frame a fundamental scientific problem, and it should avoid reliance on so-called Deep Learning or other approaches that can produce technical advances – via the computational magic of neural nets -- without revealing any deep insights. Disciplines for this topic may involve sociology, anthropology, philosophy, law, psychology, mathematics, engineering, biology, neuroscience, and computer science, among others. Innovative multidisciplinary projects are preferred.

Topic 8: Models and Methods for Understanding Covert Online Influence

This effort will provide a regional focus on attempts to use online influence maneuvers to deceive, influence, polarize, and manipulate Indo-Pacific audiences for strategic political advantage by peer states and their proxies. In many cases, covert actors are orchestrating influence campaigns to target vulnerable audiences, to make fake and deceptive information appear authoritative, and to recruit vulnerable audiences into social formations that will cause them to increasingly reject information from outside the information world of the covert actor. Technical means as well as social engineering are used in combination to achieve these effects.

Recent studies indicate that Internet-aided programs of social hysteria propagation, propaganda, disinformation, and influence operations are being conducted by covert state and non-state actors across the globe. The invasion of Ukraine and Crimea are important cases that have promoted worldwide concern. In the last three years, numerous reports on the impact of these campaigns on civil society have been published across the globe, but little is known about the pathways by which groups encounter disinformation and influence campaigns or the unique social psychology of influence in cyberspace.

Less is known about social cyber influence operations in Indo-Pacific region. There is significant evidence to show that China, as well as Russia, are actively pursuing influence campaigns in the Indo-Pacific region. Some countries are particularly riddled with bot campaigns on Twitter. Youtube, WhatsApp, Vkontatke, and other platforms are also available for developing and executing influence operations. Australia’s political parties recently found evidence of cyber-attacks on their data analysis projects, suggesting that adversarial manipulation of their elections is a growing threat.

Indo-Pacific is a large and diverse region. Therefore, it is expected that a successful effort will focus on a small collection of countries or specific topics such as elections, the Belt and Road project, anti-Western / anti-US influence campaigns, or attempts to obtain some strategic advantage for nation-state actors working through proxies.

The main objectives are: (1) to develop new theoretical understandings of the spread of propaganda, disinformation, and influence to vulnerable audiences by covert state and non-state actors in the Indo-Pacific area of responsibility; (2) to develop and validate models to assess the impact of these efforts on target communities; (3) to develop methods to assess audience vulnerability to methods and techniques of group polarization, influence, social hysteria propagation, and manipulation in the Indo-Pacific region; (4) to investigate methods to instill resilience to propaganda, deception and influence in vulnerable audiences; and (5) to investigate the specific socio-cultural dimensions and aspects of these influence campaigns and evaluate their resonance and efficacy in Indo-Pacific communities.

Social sciences, especially anthropology, sociology, computational social science, and social psychology with areal specializations in the Indo-Pacific region are recommended. Media studies and communications theory specialists are highly recommended. Information science and computer science are needed to help develop tools and models that manage up to 100,000 or more sites, accounts and make these high information flows useful and researchable by other experts.

Topic 9: Automated Cyber Vulnerability Analysis

Over the past decade, cyber assault on military, governmental and industrial networks has grown dramatically in frequency, sophistication and effectiveness. These attacks range from data theft to system denial or degradation, and their impact, whether directly on military systems, or indirectly, on the networks used by organizations contracted or sub-contracted to support the military, has the potential to compromise the effectiveness of military operations. The vulnerability of our cyber systems constitutes a critical threat to national security.

Current approaches to vulnerability assessments of information technology (IT) or operational technology (OT) infrastructure suffer from two primary limitations. First, while static and dynamic code analysis tools are critical for secure development of specific components, they cannot account for complexities arising from all possible data-input/run-time execution paths. Vulnerability scanning tools such as Nessus are useful but they only provide a snapshot in time of known vulnerabilities on a small subset of nodes where scale is limited by the number of well-trained individuals and their availability to perform the scans. Second, state-of-the-art vulnerability scanning tools focus on assessing the logical software infrastructure while largely ignoring the human element that interacts with that infrastructure. This is the case, despite the fact that most vulnerabilities are introduced through human error as exemplified by acts of omission (e.g. forgetting to close a port), commission (clicking on a phishing link), misplacement (e.g. connecting a classified machine into an unclassified network), or malicious intrusion (e.g. insider threat). The state-of-the-art vulnerability scanners are not designed to detect vulnerabilities introduced by humans interacting with the system because they contain no formal characterization of the cognitive and social behavior of the attackers. While social engineering assessments can be effective, they also require expensive involvement of experienced security professionals.

Needed are autonomous vulnerability assessment tools that can work in conjunction with human analysts to provide greater coverage of a network over more sustained periods of time. The tools should be given a logical network coverage area and then work independently to discover vulnerabilities within that area while alerting the analyst only when they find significant vulnerabilities that require immediate attention. Autonomy is necessary to reduce cognitive workload of the cybersecurity analyst so that they can focus on more operational-level tasks such as determining the most critical parts of the network to scan based on mission criticality and current threat intelligence.

This Minerva topic seeks innovative multidisciplinary research, entailing the contributions of artificial intelligence (AI) as well as behavioral, social, and statistical sciences, aimed to develop automated techniques for the assessment of network vulnerability to cyber assault along lines described above. We seek solutions with four primary features. First, they should be designed to apply to a broad range of network types, extending across scales, structural implementations, and applications. Second, because the techniques and targets of cyberattack are rapidly evolving, the solutions must be developed to be modular and capable of extensive scale-up. Third, they should be developed with the capability to uncover an extensive range of possible sources of vulnerability. Lastly, they must be informed by socio-psychological theory and analyses addressing the sources of errors in judgment that raise the vulnerability of cyber systems to attack and provide the bases for techniques to mitigate/remediate these errors.

We envision a research effort that includes an analysis of existing cyberattack databases, augmented with insights from social psychologists and both civilian and military cyber subject matter experts, to identify potential vulnerabilities and their sources. It should include development and demonstration of an executable system for automated vulnerability analysis. In addition, it should include a creditable demonstration of the validity of the system.