POC: Rebecca Goolsby, Office of Naval Research, Rebecca.goolsby@navy.mil

The use of bots as a system of message amplification to influence crowds requires a research focus on multiple issues in social cognition and computer science (and to some degree artificial intelligence) but also rhetoric and narrative. The four key techniques of disinformation: distort, dismiss, dismay, and distract (Nimmo, 2015) are reckoned to be the master set of categories in which to sort these messages. In various combinations, these tactics generate "information maneuvers" (such as group polarization, character assassination, social hysteria propagation, and manipulation of beliefs and value) that an adversary can use to move a target audience toward strategic goals. Disinformation, the deliberate creation and propagation of lies, relies on the manipulation of the social and the psychological worlds of the target audience. Disinformation campaigns are not just instances of "fake" news, but are part of larger attempts to manipulate discourse and narrative. These campaigns are most effective when they are attached to master narratives – collections of stories that are deeply embedded into the worldview, folk beliefs and values of a society. This is why campaigns that do well in one country may fail in another; effective disinformation and influence campaigns rely on attaching to master narratives which vary by culture. European scholars such as the NATO Strategic Communication Center of Excellence, refer to campaigns of disinformation and influence designed to persuade audiences by befuddling, confusing and moving them away from critical thinking as "adversarial information campaigns." The creation of "echo chambers" in online communities has also been shown to be critical to understanding why and how these campaigns are effective.

This topic would examine master narratives and their association with adversarial information campaigns in Europe. It would examine adversarial information campaigns in Europe and explore the master narratives, information maneuvers and themes to help explore what makes these campaigns compelling to their target audiences. It would examine the role of amplification, through bots, sharing activities, and other computer/online tactics in the creation of the echo chambers. It will examine why these techniques and tactics are effective, identify key features in the development of echo chambers and the creation of adversarial campaigns, and explore the current tactics in "jumping on the bandwagon" of available, potentially divisive topics to meet strategic objectives. This topic should also consider the role of cross-platform communications (such as from blogs to Twitter, Reddit and Twitter, blogs to Facebook, etc.) to consider the role of the online community in developing, validating and spreading memes and messages in an adversarial campaign and sustaining the adversarial narrative over the long term.

F. Topic 6: Automated Cyber Vulnerability Analysis

POC: Harold Hawkins, Office of Naval Research, harold.hawkins@navy.mil

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 of 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.

G. Topic 7: Power, Deterrence, Influence, and Escalation Management for Shaping Operations

POC: Martin Kruger, Office of Naval Research, martin.kruger1@navy.mil

There has been an increase in basic research on power, influence, and escalation management methodologies but a lack of empirically tested or theoretically founded decision support tools for selecting the best strategies. 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. Compared with the relative certainty and stability of the Cold War, introduction of new global threats has increased in recent years. These threats come from resurgent peers, rogue states, and international terrorist organizations. As the numbers of hot-spots increases, so do power projection, influence, and escalation management options particularly cyber risks. Examples of power projection include information warfare and cyber-attacks, action affecting economic conditions, diplomacy, and kinetic attacks. Influence and escalation management strategies include those options as threats as well as carrot and stick approaches (e.g. aid funding, Foreign Military Sales (FMS), stability force training). This topic seeks predictive models of power, influence, and/or escalation management strategies in shaping the future of a specific