Louisville KY

SOVEREIGN ACTORS MUST LISTEN TO ACADEMIC RESEARCHERS ON IMPLICATIONS OF NETWORK THEORY: OPERATIONALIZING OPEN SOCIAL MEDIA SIGNALS THE RISE OF NETWORKS AND THE CONTINUED WEAKENING OF SOVEREIGNTY

DAVID W. HENDERMAN

Prepared by:
David Henderman, CPP

02/25/2018

CONTENT

1 EXECUTIVE SUMMARY

Global civil society resides within the constructs of transnational global networks and a framework that is comprised of institutions, organizations, government actors (sovereigns) and non-government actors (NGOs). The landscape of this reality is changing. While social movement theorists have historically tracked a level of evolution of human interaction and even helped to spawn the heroic efforts of human rights activists and other NGOs serving and assisting on multiple fronts of global humanity, it seems that network theorists have identified a phenomenon that is growing and expanding at undocumented speeds.

Network theory provides a strong baseline from which to see and understand the changing global environment and a strong backdrop by which researchers can visualize and react to the effects of globalization. Globalization itself has been a miraculous phenomenon. However, as technology emergence has produced advance in transportation, trade, production, and a broad spectrum of innovation, it has also produced significant advances for those networks that may not have admirable intentions, such as transnational criminal organizations, terrorist organizations and state sovereigns wishing to impose influence through dark networks and subversive means.

Social media presents an exponential problem, rising to the level of a potential weapon of mass destruction, within the regimes of cyber space and social information networks. It lurks as a contagion that has gone unchecked and is now within the appeasement policies of sovereigns and scheduled for acceptance. Social media is an outgrowth of network theory and it must be better understood and mitigated.

2 INTRODUCTION

There seems to be a severe disconnect between academics grappling with the nuances and complexities in network theory and practitioners in defense and first response, who reside and operate within the matrix of complexities associated with both, internal and external networks in their environments. Social media has become something more than problematic, but it is not clear that the actors using it are aware of the risks associated with their current decision-making strategies. In addition, and perhaps just as concerning, is the reality that there appears to be a secondary disconnect in the space that resides between these institutions. More specifically, as it relates to network theory per se, the networks associated with academics, and then the networks associated with, we'll call it the "security community," remain disparate, and possibly, in most cases, neither realize the need for the other. It is because of this dysfunction existing within the global network, that uncivil society has begun to rise and flourish. Civil society has greatly benefited from the realization of global networks and the theories and paradigms associated with these theories have also given rise to great advance and more success in recent decades as relief organizations, NGO's (Non-Government Organizations) and other international institutions have taken on humanitarian aid advance, human rights and other global concerns, such as climate and environmental movements. However, it seems that while network theory has been advancing, there has also been a dark side associated with these advances and this dark side has given rise to a very real and present danger, that some have begun to refer to as "uncivil society."

The initial issue that appears to be driving the security community is tempo – or the speed of information, as it flows through the veins of globalized communities and institutions. Any professional having been in the security community for a reasonable amount of time would quickly admit that their agency and agencies they work with, alongside or adjacent to, are also unable to keep up. From the emergence of ISIS, to the ideas of what some believe to be called, the Arab Spring, and perhaps then, from transnational criminal organizations (TCOs) to international human trafficking networks, it seems on all front, that the "enemy" or the "bad guys" seem to be able to stay one step (perhaps more) ahead and the issues of not being able to keep up, continue to haunt those in Homeland, Law Enforcement, Emergency Management, Anti/counter terrorism, the intelligence community and even in the Department of Defense. So why is this?

There is a single issue, that we can label "tempo." However, that single issue is also surrounded by subordinate "feeders" that both are causal and resultant in nature. The first is "toxicity" and the second is "risk." This paper will identify this dynamic of tempo and provide insight into the concerns of toxicity and risk. It will identify these variables as associated with operations and

intelligence, which for the purposes of this work, it will be helpful to simplify the idea by pairing down the variables into a concept of “information sharing and collaboration.”

There is a single factor that is contributory to much of these concerns. It is called “social media.” Yet, that single concern has become a network anomaly that has begun an exponential proliferation in the last two decades. It has given rise to terms such as “going viral” and has redefined the notions of matters like “social engagement.” Both civil society, and uncivil society have learned how to capitalize on the social media network environment and use these “tools” and “operating space” in ways that those charged with enforcement have only begun to consider. There now is created a disparity between the tempo of information sharing and collaboration and the various levels of “operations.”

3 | SOCIAL MEDIA IS PROBLEMATIC FOR NETWORKS AND NATIONS

It doesn't matter if you are talking to first responders, the Federal Government, or any agency at the Department of Defense, social media is a problem. From the Intelligence Community to the Fusion Centers, information tempo drives operations and operations has been lagging behind emerging networks of what many researchers and practitioners would call "uncivil society." In terms of network theory, many academics would refer to the network components of uncivil society as "dark networks." In other words, the bad guys have networked themselves, the same as civil society organizations, non-government organizations (NGOs), and are re-framing the way "business as usual" is carried out, now on a global scale.

No one would currently oppose the notion that open social media, like Facebook, Twitter, Instagram, etc., has become an ocean of toxicity and that both information and actors are consistently suspect. So, the question becomes, "How do the good guys keep up?" There are a few reliable sources that can provide a "baseline" from which to begin to build a model for understanding the problem. As national agencies and the Defense Department begin discussions and even actions toward "operationalizing social media" (United States, Department of Homeland Security, Science and Technology Directorate 2016), there seems to be a dynamic at work, much like a siren's song, alluring decision makers into a toxic environment that will without question conclude with catastrophic results.

4 | WILLINGNESS TO COMPROMISE SECURITY FOR SPEED

Available sources indicate that these trends are emerging in all aspects of government and private sector and seem to be doing to without regard for the inherent risks involved at deeper levels of engagement, that might be recognized within the scope of data analysis, data mining, network hacking and surveillance, metadata and legacy data left behind, and risks associated with network architectures when opened to social media. A recent report by the Department of Homeland Security (DHS) openly state its intent to "operationalize social media" (United States, Department of Homeland Security, Science and Technology Directorate 2016). The implications of this intention are critical to the future of the United States. Literature on all fronts of the government and private sector state rationales that revolve around the general benefits of speedy information flow. While the details in the report provide significant insight into the future intent of government information operations, a small glimpse into those intentions and the broad-scale implications can be quickly extrapolated from the report's executive summary. What greatly complicates matters is the reality that the DHS, along with numerous other papers reside on the open internet and for all to see and to learn. This also include those who exist within the realms of uncivil society. The report states,

> Experimentation also supports the institutionalization of social media activities. To truly integrate social media into all aspects of public safety, from preparedness to response and recovery, it must be included in the following: planning and strategy development; operational and procedural documentation; legal, security, privacy, and other related policies; education, training, hiring, and exercises; evaluation and assessment; standards development; private sector collaboration and technology development; and funding strategy (both short- and long-term). Additionally, public safety agencies, especially those with legacy technology investments and long-term purchasing strategies, must consider long-term adoption and continued use of social media. This includes the need for maintaining flexibility to adapt as technology advances and internet trends change (United States, Department of Homeland Security, Science and Technology Directorate 2016, 3).

From an operations and an operations security (OPSEC) perspective, this is nearly impossible to accept as a rational documented approach to the future of public safety, and vicariously and by evidence discoverable within the literature, the defense and intelligence communities. A network

historical perspective becomes necessary to understand the roots of these problems and a willingness to admit that civil society, as well as sovereign actors may have fallen gravely behind those with perhaps, less integrity. This approach of “risk acceptance” is not highly unusual, nor does it shine light on any level of mal-intent. It does however, shine a light on contemporary willingness to compromise the integrity of government networks (social and technical) with a “hope,” that the gaps between information and operations can be repaired and overcome.

5 HISTORICAL NETWORK THEORY RELEVANCE
ANSWERS IN THE LITERATURE

To develop a roadmap to the objective, research may at this time in history have to act more as a reconnaissance into past events, than a collection of available data. It seems the targets of study and the rationales are moving. One such variable are the multiple theories associated with civil society evolving around the notion of global networks. These networks can be studies in terms of civil and "uncivil society." Both are affected by the availability of information, the accuracy of that information, but in particular, they (perhaps said "we") are all striving for the velocity at which information becomes available. This can also be described as "information tempo."

The shift in paradigms become evident by analyzing approaches advocated by Keck and Sikkink (1998) in their benchmark work, "Activists Beyond Borders, Advocacy Networks in International Politics." If this benchmark provides some level of accurate representation of contemporary global networks as they were forming in the late 1990's, then one can begin to see the evolution of the concepts as John Arquilla and his contemporaries begin to pick up the mantle of network theory, and it's evolution, related to fourth generation warfare and "swarming" (Arquilla, 2000), a term he coined to describe the more dynamic and fluid nature of networked entities as they move and relate to one another, both in context of warfare and civil society.

The evolution at first appears as a logical progression and the arguments for how global institutions and organizations form their narratives and influence regime and institutional change is fairly intuitive, and on the surface appears both reasonable and logical. The problem arises on two fronts. First, Keck and Sikkink (1998) wrote their groundbreaking work at a time when the internet was just coming into view. As an aside, one can trace the origins of network theory and find a number of authors who claim to be it's "father," or who claim to have established its baseline origins. It seems in context, perhaps it is best not to worry with that for the moment and simply acknowledge that the late 90's was associated by most academics and practitioners as a time when NGOs and other international non-government actors were also coming into view. In other words, the landscape was fluid and the future still unknown. Examine for instance the sustained disparity regarding the emergence of networks, yet within the framework and dynamics of an evolving social movement theory. Keck and Sikkink stated,

> We lack convincing studies of the sustained and specific processes through which individuals and organizations create (or resist the creation of) something resembling a global civil society. Our research leads us to believe that these interactions involve much more agency

> than a pure diffusionist perspective suggests. Even though the implications of our findings are much broader than most political scientists would admit, the findings themselves do not yet support the strong claims about an emerging global civil society. We are much more comfortable with a conception of transnational civil society as an arena of struggle, a fragmented and contested area where "the politics of transnational civil society is centrally about the way in which certain groups emerge and are legitimized (by governments, institutions, and other groups). (Keck and Sikkink 1998, 33-34)

"Activists Beyond Borders" (Keck and Sikkink 1998) is truly a remarkable work and for its time, stands as a benchmark of sorts. History can trace networks back to the turn of the 20th century with respect to labor and human rights abuses. It can go further back to the days of the resistance of slavery in the 18th and 19th centuries. One can continue back, and back, to show trade routes and conquest to the earliest days of recorded history. Yet, that is not our issue for today. But, an estate researcher would be remiss not to both identify and remain aware of the very deeply rooted systems associated with network theories and the hybrid interpretations available to the contemporary researcher. With this in mind and as a staging point, Keck and Sikkink (1998) provide modern research a stable place from which to begin. Standing on the edge of that high ground, consider Katharina Rietig's (2016) work, some 18 years later. (As an aside, it is important for the reader to be aware that now, in 2018, at the writing of this paper, even more significant advances have been made in social media technology, which continue to contribute to the problem(s) being defined. But, with that noted, it is important to remain linear in the illumination of the issue and how it possibly emerged over the last two decades.) It helps to contrast the still disconnected comprehension of NGO emergence and other related dynamics associated with adjacent theorem. Rietig also reached back to Activists Beyond Borders (Keck and Sikkink 1998), when she advanced a similar notion by stating,

> In their standard-setting work on transnational advocacy networks, Margaret Keck and Kathryn Sikkink define "transnational advocacy networks" as including "those actors working internationally on an issue, who are bound together by shared values, a common discourse, and dense exchanges of information and services." In this article, I focus on NGOs that coordinate their activities within a transnational advocacy network. They are different from social movements since they include not only activists but also lobbyists making use of their close networks to government representatives. (Rietig 2016, 271)

In the nearly two decades that span the time between Keck and Sikkink (1998), and Rietig (2016), much has changed. The Internet has taken on a much more prolific position in modern society and has also become a dependent and an interdependent variable as research begins to grapple with the dynamics of emerging social networks within the context of cyberspace. Before a brief discussion on the aspects of network theory in question, it is prudent and important to step back to the time of Keck and Sikkink (1998) one more time and take a look at a couple of the notions put forward by John Arquilla (2000). Looking at many of the same dynamics of network theory, Arquilla provides a very different, yet related visual on the dynamics of network theory by introducing the

paradigm of “swarming” (Arquilla 2000). By analyzing his work, one can clearly delineate that the same ideology was applied to a different set of variables. Thus, the knowledge transfer becomes additional or alternate, rather than inclusive. Social media then adds an added dimension that exacerbates this problem, which will be demonstrated further into this timeline of evolving network theorem. Arquilla points out,

> The key active process of the military’s work is “sustainable pulsing,” a leader force or fire. By this we mean that swarmer’s will generally take their positions in a dispersed fashion— much like U-boats on patrol. Then, they will be able to come together, concentrating their force or fire, to strike at selected targets from all directions. After a strike, they will be able to re-disperse— not only to blanket the battle space but also to mitigate the risk posed by enemy countermeasures— ready to “pulse” to the attack again, as circumstances permit. This should not be thought of as a strictly military phenomenon. Sustainable pulsing can be undertaken in social action as well. (Arquilla and Ronfeldt 2000, 21-22)

The last notion that “pulsing can be undertaken in social action as well” (Arquilla 2000) is critical. The idea that these network theories are running parallels in time, while applied to different global applications is not problematic, until the dynamics of social media are applied, which not only capitalize on the notion of “sustainable pulsing” (Arquilla 2000), but then evolve into a systemic form of force multipliers that can be applied on multiple fronts and multiple tiers.

The idea of “information toxicity” begins to form as the identification of actors is transformed, mutated and concealed. “Sustained pulsing” over time can become “viral” or worse. Because the network loses its structure and deliberate topology, information can now become not only asymmetric, but omni-symmetrical, which reaches back to the roots of realism within the context of chaos. There is a kind of paradox at play here, in that the network becomes so chaotic, that it ceases to be a network at all and information, good or bad, has literally become injected into cyberspace where “nodes” reach and grab and either stop or propel that information into their own subnetworks, literally adding to the function of information chaos. Generally, in terms of social intelligence theories, group dynamics come into play in these networks initially, but with anarchical pulsing have the propensity to create chaos, rather than results. This in theory represents “toxicity” in the network of social media. This explanation is only a surface level evaluation, but it represents a gap in archival and contemporary research. In terms of social media networks, and the government’s desire to “operationalize social media” (United States, Department of Homeland Security, Science and Technology Directorate 2016), this notion of toxicity is only a subset of issues associated with the desire to control information tempo and operational dominance via the constraints associated with cyberspace.

In 2009, Dr. Arquilla gave a seminar at USC Annenberg, School for Communication. The class was focused on network theory, but there were a couple of items that were demonstrated as problematic and that add to the supposition in this paper, that conflicting ideologies and terminologies existing, even in terms of recent years, continue to exhibit the fact that network theory is evolving at a pace

that research has not kept up, and perhaps demonstrate a signal in time that a new paradigm must be identified; associated specifically within the constructs of network theory, but specific and focused on the dynamics associated with social media and emerging similar networking technologies.

Essentially, Dr. Arquilla diagramed and explained to the class that in network theory, we also recognize the roots of realism, liberalism and socialist theories. He discussed the paradigms, units of analysis and the state of nature in all three theories. He then identified a fourth "theory," but did so loosely and referred to it as "syndicalism." The unit of analysis was the network, but his state of nature was what he referred to as "panarchy." He stated that he and his partner, David Ronfeldt had coined the terms and provided the class a brief description of their meaning (Arquilla 2009, https://www.youtube.com/watch?v=xfr8LX9RO10&feature=youtu.be). The issue at hand is that a quick study of the terms provides additional and conflicting information. The ideas and notions of Arquilla's work and approach in this seminar were overall, generally brilliant, as usual. However, this divergence from traditional norms associated with network theory seemed to signal shaky footing on current evolutions and developments within the framework. Once again, this also possibly signals an existing gap in not only the research, but also in the network relationships existing between academics and practitioners. Perhaps it is important to note that Dr. Arquilla identified that the United States has been attempting to fight terrorism through a realism paradigm, when in fact, terrorist organizations exist within the context of network structures (Arquilla 2009, https://www.youtube.com/watch?v=xfr8LX9RO10&feature=youtu.be). His points were well made, however, the gap that exists along this network theory timeline, from the late 1990's to 2009, when that seminar was delivered, remain a gap today. That gap is exacerbated by the proliferation of social media and remains ever widening because of the increasing tempo at which information has been enabled to proliferate.

In 1998, David Ronfeldt and John Arquilla authored a critically important paper on the Zapatista movement in Mexico. They clearly demonstrate the rise of the Internet and its influence and impact in social struggle, which they coin he term "Netwar." (Ronfeldt and Arquilla 1998). Their use of network theory associated here runs alongside of Keck and Sikkink (1998) and provides a good place in time and history to see where the trajectory of ideas begins to split. Whereas, Keck and Sikkink (1998) provide keen insights and a strong foundational knowledge regarding influence, regime change and framing of issues, Ronfeldt and Arquilla (1998) provide a framework for engagement on a different level focused on warfare and force, which would begin a slow change as the future unfolded. It might be said that social engagement in terms of global civil society is better suited to benefit and both manipulate and command the use of social media as it relates to global engagement. On the other hand, military and security operations are not necessarily equipped or positioned to operate within such a chaotic and non-secure environment.

6 THE ALLURE OF OPEN SOCIAL MEDIA IS NOT WORTH THE RISK

Security becomes an issue, as does mission focus and creep. Contemporary social media, while a high-speed tool and environment for communications was developed and is still currently operated by private corporations and international corporations that may or may not (usually not) share the same or similar interests or agendas as state actors, or the institutions that represent them. Today, literally within the last couple of decades, the Internet has helped both parallel paths to move rapidly forward. However, in recent days, operations associated with state security have begun to be jeopardized by a "pulling away" of entities not restricted by law or regulations. This disparity of tempo has become problematic for government agencies all around the globe, but particularly for the United States, where free speech and other civil protections allow individual nodes with the network to act generally without restrictions. In short, the implications of social media in network theory, as it relates to government institutions and state actors is perhaps, widely different, than it is for NGO's, transnational civil institutions and other bad actors, such as transnational criminal organizations or even terrorist networks. Herein, is a major gap in both the research, and the point of the network structure where "bridges" may be constructed.

Understanding the inherent risks associated with network topologies and a principle referred to as the "Small World Theory," or "Six Degrees of Separation," can help practitioners not only understand risks associated with proximity to "network toxins," but also provide a mutual place for discussion between operations and intelligence, as it relates to social media. The more random the node-connections (which is common to individual networks in social media), the more powerful the actual reach of connected nodes. Recent discussions have begun to center around the idea that social media has contributed to this principle of connectivity to the degree that the principle that has been around for more than a century is actually beginning to drop to five and possibly four. Understanding the basis for this proposition in simple terms can be understood by the security community with respect to the distance between civil society and uncivil society, which appears to be decreasing as network technologies advance. While this is a simple illustration for representing a theory within network topologies, it also represents a segment of the rationale as to why government approach to understanding social media becomes a matter of global security, in addition to a sociological paradigm. Specific to networks and social media risks, these concerns create significant risks when decision

makers conveniently decide to occupy space within the institutions of open and non-secure social media environments.

There is a key finding in the Zapatista study (Ronfeldt and Arquilla 1998), that is now relevant, perhaps in a cyclic way. The authors note that the evolution of what they termed “netwar” had begun in actuality, some two to three decades before this Mexican conflict began. They further drew the conclusion in the study in general, that these dynamics were significant, to the level of changing the entire tempo and topology of both networked organizations, but also the resulting effects of their strategies. Ronfeldt, who was the lead on this project stated,

> This swarming by a large multitude of militant NGOs in response to a distant upheaval—the first major case anywhere—was no anomaly. It drew on two to three decades of relatively unnoticed organizational and technological changes around the world that meant the information revolution was altering the context and conduct of social conflict. Because of this, the NGOs were able to form into highly networked, loosely coordinated, cross-border coalitions to wage an information-age social netwar that would constrain the Mexican government and assist the EZLN’s cause. (Ronfeldt and Arquilla 1998, 3)

Key focal points that apply to this issue of information tempo today are noted. Historically, these researchers, while still in line with Keck and Sikkink (1998) put forth the notion that the changes in networking and operations had actually begun some twenty to thirty years before the actual events took place. It is in this same context that social media has begun an evolutionary change to networks in contemporary terms. Yet, this study theorizes that it is very likely that government, and/or state actors, or maybe even differently stated, the interests of sovereignty have overlooked the long-term effects of social media with respect to lost tempo and context of available information sources.

7 CONTEMPORANEOUS HISTORY PROVIDES INSIGHT TO SOLUTIONS

These rising dynamics are critical for government to understand and to act appropriately, which generally means with an educated rationale, as opposed to an emotional response that seeks to fill a deficit of time in the space of information sharing. There is indeed a gap, and many practitioners in governmental contexts have identified it. What is to be done about the gap is altogether a different matter and there seems to be a very loosely defined approach that appears to align itself with embracing the chaos, rather than slowing down in a form of tactical retreat, regrouping and managing the deficit with reason and science. The risks are clear and to remain within the ecosystem and ethos developed by Dr. Arquilla, it might be helpful to contemplate his warnings documented in his paper published in the Brown Journal of World Affairs in 2007. Referring to networks, he intimated, “whether networks are representative of civil or uncivil society, their actions are often serious attempts to keep the world system from being unduly controlled by the pre-eminent national powers of our time” (Arquilla 2007, 205). He ends the discussion with this dark warning, “In truth, if a protracted “netwar” comes to dominate the twenty-first century landscape, it will be highly unlikely that nations will emerge as the victors. This is all the more reason for us to take networks seriously now—to incorporate them into our highest orders of thought about the world system, and to embrace them fully as partners in the great policy deliberations of our time” (Arquilla 2007, 208).

For this to become a reality, government must not only take seriously rapidly evolving network theory, but, must begin to metaphorically analyze social media in its relationships to network theory, and similarly illustrating the point, as artificial intelligence is aligned relationally to generalized computing. While a type of force multiplier, social media is also a network organism that has proven time, and again, that it is capable of spinning off, or spinning up, viral information contagion, both deliberately, and by chance, with little to no probability of prediction. As Dr. Arquilla often notes, these matters of discussion and study carry with them significant gravity for those who will hear them. They have demonstrated the ability to cripple and transform nations when left unattended.

8 A WILLINGNESS TO LISTEN AND UNDERSTAND MARKS THE PLACE TO BEGIN

"Listening" is a social technique and skill, not performed well by most sovereign actors. It will become a necessity and to build on and illustrate Arquilla's concluding remarks noted above, Gupta and Brooks (2013) write,

> But in recent years, thoughts and discussion surrounding social media have led to heavy subjects such as revolutions in the Middle East and riots in the West. The 2011 Arab Spring and 2011 London riots are controversial, yet powerful examples of how social media is impacting matters of security. Activists and individuals globally have begun using social media as a way to connect with each other, amplify their voices, coordinate actions against government and law enforcement, and publicize their side of the story - actions that have changed the world. (Gupta and Brooks 2013, 4)

All is not lost, but not heeding the warnings of those researchers who have clearly identified the historical roots of a very contemporary problem may end with the downfall of a free world. Perhaps the United States, as a global power will either learn to listen to available research and plan accordingly, or the lessons of the events like the Zapatista movement in Mexico, the Arab Spring in Tunisia, riots in London and around the world will fall on deaf ears. The great sovereigns that view themselves through hegemonic worldviews and as the "protectors" of the world, may find themselves toppled by a network phenomenon called "social media." History speaks of such events. The real key to asking the right question may be, how can academics cause practitioners to listen?

9 CONCLUSION

The works of John Arquilla and David Ronfeldt have been sounding the alarm for nearly two decades. Interestingly, their early ideas also postulated that predictive information had been available to the documented rise of networks some twenty to thirty years before that. (Arqullia and Ronfeldt 1998). Their work is only one path of research and not the only resource. However, for this discussion regarding security risks, their platform makes for a good benchmark. While it seems that leaders are not listening, there may be hope in the idea that researchers might take this a watchman's responsibility to change tactics for being heard. Those providing information and consultation to the Department of Homeland Security have not based their opinions and consultation in scientific method or approach. They represent a "hit and miss" approach to best practices and a "hopeful" approach to identifying some things that have worked and some that have not. This is not sound science, nor is it a way to solve the issues associated with rising dark networks (within the constructs of open social media) or the toxic and lethal risks associated with open social media engagement at an operational level.

A great threat to nations and sovereignty exists within the constructs of network theory. Contemporary leaders do not seem to be paying close, if any attention, to available academic research that suggests that sovereignty is in jeopardy and that globalization, aided by the rise of the Internet and other technological advance is at the heart of what amounts to an unseen revolution. Social media presents an additional layer of complexity to the already complex and ever evolving power of global networks, especially those that would seek to reframe regimes and topple actors, that have historically constructed influence within the contexts of hegemony.

Social media and the interlaced technologies that define themselves within the Internet of Things (IoT) play a significant role as a dynamic force multiplier and have in recent years proven the ability to outpace and outmaneuver the best of the best in terms of operations, special operations and the best and brightest of the intelligence communities, to provide only one such example. From events well known to all like the attacks on New York on September 11th, 2001 to the devastation of Hurricane Katrina, time and again, history has taught that sovereign powers are not listening. The information was there and available such as to allow prevention and proactive engagement. Yet, leaders and decision makers cognitively chose to ignore or avoid the research. Network theory is no different.

The rise of the power of global social networks can not be ignored by those intent on maintaining some reasonable level of order. Sovereignty is indeed in jeopardy, yet, perhaps something more sinister is the question of what happens after the shear force of networks topples the existing order and infrastructure that provides stability in the current world? Social media is a growing concern that has been greatly ignored. Even within the constructs of “operationalizing” it, both government and corporations have ignored the inherent risks associated with an environment in cyberspace that has no tangible bounds and that remains not under the control of sovereign actors, but as a “power tool” of sorts in the hands of those who may or may not have the best interests of the state or the individual in mind.

Rather than paying attention to the ideology of networks and seeking how state actors might align and build relational networks to support and frame existing sovereignty, it remains clear that decision makers have resigned to remain in a posture of hegemonic sovereignty, perhaps visualized as “stiff necked” while at the same time accepting the regime of social media as it was defined by actors motivated by financial gain. It may not be that this is a deliberate acceptance, but it glistens with the same façade - “ish” notions that France embraced within the context of deliberate appeasement policies during World War II. Most would remember from basic history class, that France was quickly overwhelmed and struck down by an enemy she refused to acknowledge.

Network theory research is vast and provides all of the knowledge and tools necessary to see and understand the dynamics associated with transnational global networks. Even within the context of available literature, it is likely that enough information and expertise currently exist to address the rising problem of social media. This study concludes that open social media may represent a type of weapon of mass destruction within the regimes of cyberspace. Those intent on setting it off, within the constructs of defiant global networks continue to experiment and press the agendas, literally within plain site of hegemony and sovereignty. Acceptance of social media as it currently exists today, without any form of inertia to resist uncontrolled growth and unprecedented expansion will without doubt result in a changing of the face of global civilization, as well as global civil society.

10 RECOMMENDATIONS

It is recommended that researchers develop and present a comprehensive risk assessment and seek proper funding to support the development of secure approaches to mitigating the effects of social media, as this is the first and greatest threat resulting from evolving global networks. A scientific and competent approach to this initiative should be defined and specified in planning, and a roadmap developed by a hybrid and high-level team of professionals. Planners or researchers chosen because they have a knowledge of how to use social media effectively is not the right approach.

Research a'nd development must be given to the creation of secure government networks that allow for the same or greater information tempo, in support of information sharing and collaboration that is experienced by all actors on open social media. Proper and appropriate policy should be developed to support such an infrastructure. Education for first responders should be developed that explain in layman's terms the inherent risks of associated focused operational matters within the confined global social environments of privately owned, open social media, as well as by persons who "live" on the "backend" of the networks. Access to meta data, trends, intentions, plans, locations, agent demographic information, etc. are only a few of the known risks associated with this approach. The world literally has become smaller and global actors civil and otherwise have access and visibility to local matters. Distance has literally been removed from the equation of connecting nodes.

A methodology should be developed, whereby, first responders do not seek to "operationalize," in other words, operate within the operational environment of open social media. Risk in OPSEC, INFOSEC and general security exist, and it is less than prudent to expose agencies or individuals to these levels of security risks.

A proper understanding by first responders and defense professionals should be developed by education and training, to support the proper engagement of open social media. In other words, information, whether for use in adversarial roles or emergency management should be collected, assessed and disseminated with proper and secure protocols. If a paradigm shift could be instituted that moved government and companies into safer spaces and allowed them to develop what some are beginning to call "interest networks," it may be possible to change the momentum and influence, or at least slow it down, with respect to current trends in open social environments. Operational collaboration, other than generally communicating with the public is a catastrophic security event waiting to happen. This of course does not take into account the absolute necessity of analysis of social media as an operational space, which is very different than operating within

that space.

Lastly, government entities, particularly at the local level need to begin to consider their outward facing approach to the public and how to facilitate this without deep presence within the open social environment. It is likely that the positioning of community social networks that are secure and controlled could produce a much better collection platform, along with helping to focus information and culling out much of the “noise” during critical times. Network theory and all of the available research has taught us a lot. However, the current approach to social media will result in far greater catastrophic events than the ones agencies believe they are preparing to support.

REFERENCES

Arquilla, John and David Ronfeldt 2000. Swarming and the Future of Conflict. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/documented_briefings/DB311.html.

Arquilla, John and David Ronfeldt 2001. Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/monograph_reports/MR1382.html.

Arquilla, John 2007. Of Networks and Nations. https://www.brown.edu/initiatives/journal-world-affairs/sites/brown.edu.initiatives.journal-world-affairs/files/private/articles/14.1_Arquilla.pdf

Arquilla, John, "Annenberg Neworks Network Theory Seminar" (lecture, USC Annenberg School for Communication, March 24, 2009). https://www.youtube.com/watch?v=xfr8LX9RO10&feature=youtu.be.
Gupta, R., Brooks, H. 2013. Using Social Media for Global Security. Indianapolis, IN., John Wiley & Sons, Inc.

Keck, Margaret E., and Sikkink, Kathryn. 1998. Activists Beyond Borders: Advocacy Networks in International Politics. Ithaca: Cornell University Press.

Rietig, Katharina. 2016. "The Power of Strategy: Environmental NGO Influence in International Climate Negotiations." Global Governance 22, no. 2: 269-288.

Ronfeldt, David, John Arquilla, Graham Fuller, and Melissa Fuller. 1998. The Zapatista "Social Netwar" in Mexico. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/monograph_reports/MR994.html.

United States, Department of Homeland Security, Science and Technology Directorate, DHS Virtual Social Media Working Group and DHS First Responders Group, From Concept to Reality: Operationalizing Social Media for Preparedness, Response and Recovery, April 2016, https://www.hsdl.org/?view&did=792751.