Identifying Agile Security Patterns in Adversarial Stigmergic Systems

Jena Lugosky
L-3 Communications
dagnyruns@sbcglobal.net

Rick Dove
Stevens Institute of Technology
rick.dove@stevens.edu

Copyright © 2011 by Jena Lugosky and Rick Dove. Published and used by INCOSE with permission.

Abstract. System adversarial communities appear to exhibit characteristics of natural agile systems, and enjoy an advantage as a result over static systems that are the focus of their attacks. A project started in graduate courses at Stevens Institute of Technology and currently pursued by the International Council on Systems Engineering Working Group on Systems Security Engineering works under the premise that security strategy will benefit by architectural patterns that are equally self organizing. To that end a pattern cataloging project is in process, identifying fundamental self organizing patterns that can explain the adversary operational modes and inform next generation security strategy. This article advances that pattern project by exploring and capturing the stigmergic communication employed by system-adversarial communities according to the pattern project guidelines. This article first identifies the unique stigmergic pattern, explores its nuances, and presents it in a format identified by the pattern project. Then the stigmergic pattern is applied as a mold to analyze a series of three systems in an effort to regard each within a familiar context. Three adversarial systems, the Iraqi Insurgency, IED Networks and Cybercrime, were selected as prominent opponents that provide significant consternation to security experts. They are first identified as agile systems, per characteristics defined by the pattern project, then studied in the context of the stigmergic pattern.

Introduction

As we move into the 21st century and realize the implications of a truly interconnected global community, the importance of understanding and claiming responsibility for our security grows. Collectively we dabble in deceptively complex systems that present peril for which we, individually and as a Nation, are ill prepared. The adversary who successfully survives current security practices is agile, often well-funded, and a consummate foe. China houses an extensive, proactive hacker community, that is well known for its "willingness to engage in large-scale politically motivated denial of service attacks, data destruction and Web defacements of foreign networks". In 2001, the collision of a US Navy EP-3 reconnaissance plane and the People's Liberation Army Navy F-8 fighter, initiated the first "Sino-US Hacker War," that included, "denial of service attacks and Web defacements launched from both sides against government and private sties" (Bryan 2009). As the fight in Iraq continues, the United States and its allies have fielded the most advanced and complex weaponry ever developed. Despite these valiant efforts, the war has yet to be won. In 2009, IEDs accounted for nearly 60% of coalition battle deaths in Afghanistan, killing 275 troops. In Iraq, insurgents were planting up to roughly 4000 IEDs a month in that same timeframe (Dreazen 2009). The enormity of the problem is striking and demands attention. Our collective attempts to secure our borders and our freedoms are demonstratively at risk.

A pattern project started at Stevens Institute of Technology's School of Systems and Enterprises, and now also being developed by the INCOSE System Security Engineering Working Group, is cataloging examples of fundamental self-organizing security patterns. The purpose is to provide a better understanding of the adversary strategies and operational modes, and develop architectural patterns for a next generation of security strategies. The work seeks to categorize self organizing agile security patterns to facilitate communication and understanding between System Engineers, Security Engineers, and Leadership to facilitate security system discussion and development.

Six characteristics of self organizing adversarial communities have been identified, with the expectation that next generation security must at least provide parity with the agility of intelligent attacking systems (Dove 2010a, Dove 2010b). These six characteristics are summarized in Table 1, and are referred to as the SAREPH characteristics. Guidelines currently employed on the pattern project for nominating candidate patterns for the catalog are:

- The system must manifest both the self-organizing characteristic and the harmonious characteristic.
- The system must manifest the evolving characteristic and/or the adaptive characteristic.
- The system must manifest the proactive characteristic and/or the reactive characteristic.

Table 1 Pattern qualification filters

[S] Self-organizing—with humans embedded in the loop, or with systemic mechanisms.
[A] Adapting to unpredictable situations—with reconfigurable, readily employed resources.
[R] Reactively resilient—able to continue, perhaps at reduced functionality, while recovering.
[E] Evolving with a changing environment—driven by situation and fitness evaluation.
[P] Proactively innovative—acting preemptively, perhaps unpredictably, to gain advantage.
[H] Harmonious with system purpose—aiding rather than degrading system/user productivity.

This article first identifies the unique stigmergic pattern, explores its nuances, and presents it in a format identified by the pattern project. Then the stigmergic pattern is applied as a mold to analyze a series of three systems in an effort to regard each within a familiar context. Three adversarial systems, the Iraqi Insurgency, IED Networks and Cybercrime, were selected as prominent opponents that provide significant consternation to security experts. They are first identified as agile systems, per characteristics defined by the pattern project, then studied in the context of the stigmergic pattern.

The Stigmergic Pattern

Pattern Introduction

Any stigmergic system is comprised of a population of agents and their defined environment. Stigmergy is the process of indirect agent-agent communication through the environment that

serves to coordinate seemingly intelligent collective action. Each agent is defined by (Parunak 2005a) as having:

- an internal state, which generally is not directly visible to other agents;
- sensors that give it access to some of the environment's state variables;
- actuators that enable it to change some of the environment's state variables;
- a program (its "dynamics") that maps from its current internal state and the readings of its sensors to changes in its internal state and commands given to its sensors and actuators.

Notably, the agents are not necessarily able to sense all signals presented in the environment. Additionally, the agents vary in their ability to perceive, interact and react to the environment. The environment is defined by (Parunak 2005b) as:

- a state, aspects of which generally are visible to the agents;
- a program (its "dynamics") that governs the evolution of its state over time

"The most important distinction between agents and the environment is that the internal state of agents is hidden, while the state of the environment is accessible to an agent with appropriate sensors" (Parunak 2005b). Each agent can be conceived as a discrete unit, or as a self-contained object with a well-defined boundary. The environment is a localized shared problem space defined by its structure and dynamics where the agents interact indirectly.

The beauty of the stigmergic pattern is perhaps its universal simplicity. Stigmergy is manifested in the form of Figure 1.

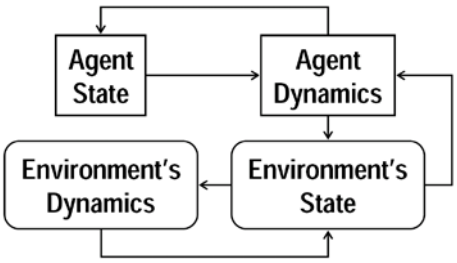


Figure 1 Basic Architecture of Stigmergy (Parunak 2005b)

The agent state is comprised of the agent's physical, physiological, and emotional being as well as all those historical and cultural experiences that integrate to form the agent's experience of self. It is the confluence of events that together influence the agent's perception and comprehension of the world, and in turn filter the observation of the agent's surroundings. It is through this filter that a given environment state communicates different information to diverse agents. Though the environment's state is objective, the agent's realized internalization is subjective. In any stigmergic encounter, that agent state combined with the perceived environment influence the agent's action on the physical environment—the environment is altered. A trace of the agent remains, in the form of the altered environment (a new environment state), which serves as a signal for one or more succeeding agents to process. The agent's response is dependent on both the agent's state and the filtered environment state, such that each agent behaves distinctly.

The stigmergic variety is integral to the interaction between the agent dynamics and the

environment state. In *marker-based* behavior, the agent leaves its signature on its surroundings (intentionally or not), to signal to another agent. In s*ematectonic* stigmergy, the agent responds to a signal in the environment, either knowingly or unwittingly. So to complete a stigmergic cycle the environment is changed by an agent, then that change influences the behavior of another—first with marker-based then with sematectonic stigmergy. And the cycle continues if the sematectonic response includes leaving a mark on the surroundings.

A further classification breakdown distinguishes between qualitative and quantitative signaling. Qualitative refers to a variable *nature* of the signal. In *qualitative marker-based* stigmergy ants react to nature of the pheromone-trail chemistry, and in *qualitative sematectonic* stigmergy nest-building wasps react to the nature of the structure already in place. Quantitative refers to the amount of signal present in the environment – in *quantitative marker-base* stigmergy ants favor a trail with more pheromone over an alternate trail with less, and in *quantitative sematectonic* stigmergy ants move dead ants from a smaller pile to a larger pile.

Significantly, in stigmergy the response is indeterminable—there is no direct feedback to resolve the response to a determined form. Genetics and probability guide expectations, but the factor of the unknown agent-state inserts a level of uncertainty that is critical to the control and manipulation of this pattern of stigmergy.

SAREPH Characteristics

This section examines how the stigmergic pattern manifests each of the six SAREPH characteristics, so called for the first letter of each characteristic outlined in (Dove 2010a and Dove 2010b).

Self-Organization – A key component to any stigmergic system is the occurrence of self-organizing behavior that results from the uncertainty inherent in indirect communication. The intelligence which drives organization, "resides not in a single distinguished agent (as in the centralized model) nor in each individual agent (the intelligent agent mode), but in the interactions among the agents and the shared dynamical environment" (Parunak 2005). The meaning of signals and the control of the system is distributed (decentralized) among the agents. Stigmergy's indirect communication attribute allows harmonious action of the agents without a overarching centralized plan.

Adaptable Tactics – Adaptability is enabled by an inventory or immediate acquisition of appropriate resources. The resources available for marker deployment and response action in the environment are virtually limitless and ever adaptable. When one signal fails to communicate and generate the desired response, another method may be employed. If the expected action is unavailable or limited, another might fulfill its purpose.

Reactive Resilience – The two tangible components of stigmergy that can be disrupted are the agent and the environment. If the environment is compromised, the agents will continue to pursue their tasks, and again, purposefully or inadvertently, leave behind traces in their efforts. If the agent population is marginalized, the remaining survivors would benefit in demonstrating (teaching) the stigmergic mechanisms (signs and their meaning) as the population is reestablished. Additionally, the meaning of signals might be eradicated, or confused, so as to lose their effectiveness. But it is in the nature of agents to respond to the environment, and as such new traces

will emerge, with accompanying anticipated behavior.

Evolvable Strategies – Stigmergic change in the environment is for all agents to interpret and act upon, encouraging a multitude of appropriate responses that are filtered by each agent's state. Since the response is indeterminate, evolution is inevitable. Each response is slightly different, with those invoking the sought outcome becoming favored. Over time the meaning of a sign, and the expected action evolve to initiate a different expected action.

Likewise, because stigmergy is "directed at the shared environment, it will gradually reshape this medium into a structure that supports increasingly efficient and synergetic interactions," (Heylighen 2007).

Proactive Innovation – Proactive innovation is a potential aspect of the fundamental stigmergic act of an agent responding to a change in the environment. In the manner of another pattern identified in this project, *horizontal meme transfer* (Dove 2010b), the agent may adapt if so inclined ideas from other domains to respond in an innovative manner. Likewise, the agent may draw upon parallel experiences of another agent to understand and respond to an unfamiliar environment state. In both cases, the agent is using material that is not integral to the circumstance to adjust the response unpredictably to gain an advantage in the situation.

Harmonious Operation – Inherently, stigmergy is harmonious. Contradictory and inharmonious signals result in uncertainty and confusion. Stigmergy is often enacted without the direct knowledge of either or both of the agents, so integrated it is into the ways of the agents. Again, Parunak notes when agents are human that "it would be more difficult to show a functioning human institution that is not stigmergic, than it is to find examples of human stigmergy" (Paranuk 2005b). It is so common we do not notice it, yet it molds our lives. Traffic signals, internet forums, office bulletin boards, home décor—it is present in every way humans modify the environment to communicate or relay expected behavior.

Table 2 shows an initial version of the stigmergic pattern presented in the format adopted by the SAREPH pattern project, with a very general graphic reflecting a qualitative sematectonic stigmergic change in the environment caused by one agent that affects the action of another agent. Further work will develop a graphic for all four variations of stigmergy.

Adversarial Stigmergic Patterns

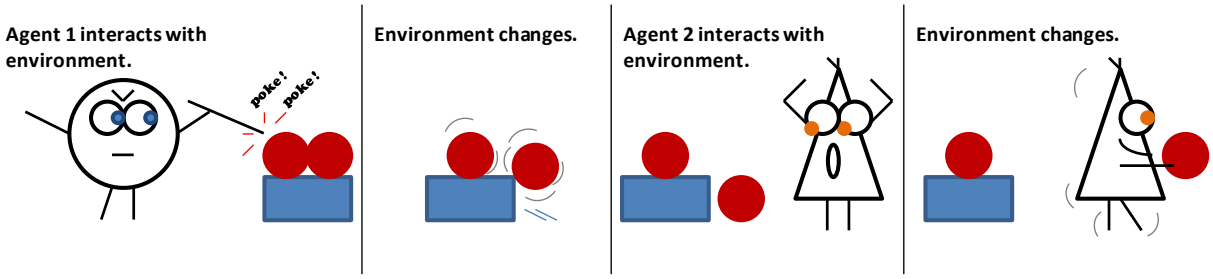
To further the work of the SAREPH pattern project in identifying and categorizing examples, this section demonstrates how the behavior of the Iraqi Insurgency, IED Networks, and Cybercrime follow the stigmergic pattern defined previously. In each case we examine how the SAREPH characteristics represent the core of attacker agility, as the project proposes, and then explore how indirect communication via the environmental medium is employed by each.

Iraqi Insurgency

The myriad of websites dedicated to the *jihad* are stigmergic traces of an agile, technically savvy, and politically astute Iraqi Insurgency that acts deftly on trails left by the work of others. The Internet provides anonymity and security to those who seek to spread their message without reprisal, to bolster public support, amass followers, petition funding, or simply chronicle their

discoveries and knowledge. It allows the many disparate ideologies that comprise the insurgency to communicate indirectly and influence relentless innovation toward realization of cause.

Table 2 Stigmergic Coordination Pattern Form

Name: Stigmergic Coordination (agent response to traces in the environment.)
Context: Indirect environment-mediated communication (Elliott 2006). Traces left in the environment by one agent incite an action of another agent.
Problem: A need to communicate effectively, but indirectly.
Forces: Strength of the signal: dispersion to signal large area vs. evaporating/dissipating signal fades over time. Agent population: robust populace vs. diverse set of agents with individual signal interpretation causes inherent uncertainty. Form structured (self-organizing) become rigid and inadaptable.
Solution: Recognize and command the inherent possibilities for indirect communication available in the manipulation and modification of the surrounding environment. The generic stigmergic pattern is supplemented by four sub-patterns that further classify interaction: (marker-based, sematectonic, qualitative, quantitative).
 A general depiction of qualitative sematectonic stigmergy.
Example: Ant colony forging (Parunak 2003) **Example:** Ant colony corpse gathering (Beckers 1994) **Example:** Wasp nest building (Parunak 2005b) **Example:** Human-human internet use (Parunak 2005b)
Agility: Self-organization results from the uncertainty inherent in the system's stigmergic communication. Adaptation of signals occurs to adjust the response. Reactive resilience sustains signal meaning and communication norms for a given agent population. Evolution is driven by the multitude of individual agent states and unique filters. Proactive innovation occurs as parallel resources are incorporated in response to an unfamiliar environment state. Harmony underlies the integration of stigmergic communication into everyday interactions. [SAREPH]
References: (see reference section, only URLs shown here (Parunak 2003) www.newvectors.net/staff/parunakv/msh03.pdf (Parunak 2005b) www.newvectors.net/staff/parunakv/E4MAS05HHS.pdf (Beckers 1994) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.117.568&rep=rep1&type=pdf

One aspect of identifying the Iraqi Insurgency as an example of the Stigmergic Coordination Pattern is demonstrating that it too embodies agility as presented in the SAREPH characteristics

and guidelines; true for all three examples:

- The system must manifest both the self-organizing characteristic and the harmonious characteristic.
- The system must manifest the evolving characteristic and/or the adaptive characteristic.
- The system must manifest the proactive characteristic and/or the reactive characteristic.

Self-Organization – This is the most significant tenant of the Iraqi Insurgency. A multitude of different factions driven by diverse tribal histories, interests, loyalties, and beliefs have found effective stigmergic communication of their cause through guerilla tactics. These diverse organizations, traditionally consumed with internal conflict, have effectively self-organized to demonstrate through kidnappings, brutal murders, sniper attacks and IED bombings their collective opposition to the coalition forces and mission. Dubbed, 'open-source warfare' for its resemblance to the open-source software hacker mentality, it is hallmarked by nonhierarchical networks and collaborative efforts to achieve a common purpose (Robb 2007). The indirect communication of effective disruption via television, internet forums and websites, or public uncertainty and mood, goad other agents into related action, and the stigmergic cycle is fueled. Michael Doran, the US Deputy Assistant Secretary of Defense, explains that, "networks such as Al Qaeda use the Internet for a variety of organizational purposes, including recruitment and fund raising" (Adhami 2007). Videos portraying accomplishments of the insurgency are presented to gather popular support. There is no one overall leader who directs operations for the insurgency, but each faction acts of its own accord and motives (Robb 2009). A host of internet forums are the melting pot for stigmergic influence on strategy, tactics and purpose. "Websites are used to announce new policy positions, alliances or strategic shifts, react to breaking news, or comment on how the Western media is addressing the struggle"(ICG 2006). Fighters and supporters alike exchange, in posted dialogue, thoughts on the nature of the conflict, lessons learned and information about new techniques for the construction and handling of explosive devices.

Adaptable Tactics – The use of adaptable tactics is a particularly effective and key component of the insurgency's capability. One sect's effective transgression spurs others to adapt the successful tactic. When coalition forces neutralize a method, the media seizes it and announces this shift in the environment—and the enemy, alerted, alters its game. For example, security services work tirelessly to interrupt message dissemination by terminating *jihadi* websites. Website administrators exhibit "impressive skills at adaptation", in relentlessly relocating the content to other servers, ensuring the information remains available to support the cause (Adhami 2007).

Reactive Resilience – The unrest in the Middle East has continued throughout history. The resilient quality of the insurgency is evidenced in its persistence in the region—probably driven by unresolved deep seated issues, a seemingly unending replacement of eradicated resources, and the increasing access to ever-affordable technologies that can replace and improve upon technical countermeasures. As radical Muslim scholars spread their message worldwide on mainstream Islamic websites, giving voice to the ongoing "war on Islam", they reach to include those that are well removed from direct suffering, to ensure continued dissonance. With this perpetuation, scandals such as Abu Ghraib, and the Mahmudiya massacres continue to resound, arousing anger and frustration throughout the worldwide Muslim community (Adhami 2007). Other websites target Muslim immigrants in the western world, where many immigrants exist at the fringes of society and feel marginalized by the European mainstream. The media purports that "European

governments are rejecting them because of their Muslim identity" (Adhami 2007), undeniably spurring anger and resentment in support of the "war on Islam" theory. If the purpose of the insurgency is to maintain that uncertainty, they are building upon a long tradition of success.

Evolvable Strategies – Over the course of the conflict the insurgent strategies have evolved to meet the shifting face of the environment. They began as many small factions, then via the internet, aligned their vectors to the common jihad. "Progressively, as a result of fierce competition, smaller, less effective groups disappeared or merged with more successful, well-established and prestigious ones, such as Tandhim al-Qa'ida, Jaysh Ansar al-Sunna and al-Jaysh al-Islami fil-'Iraq. By 2005, what had begun as an assortment of isolated cells thus became a set of far wider and sophisticated networks" (ICG 2006). They became more effective once infighting was mitigated and efforts were focused on the *jihadi* cause. Communication, via internet forums increased coordination among factions, and political tactics have progressed. Most significantly from a stigmergic sense, the insurgency learned from its own mistakes and changes in the coalition's tactics, as they were communicated via Internet sites, and modified its behavior to reflect the new environment (ICG 2006).

Proactive Innovation – Time and again, the Iraqi insurgency has innovated to maintain an advantage over their enemy. As the environment has changed, their responses have been creative, unexpected, and at times have exceeded expectations in their brutality and in their use of new technologies. The focus of the insurgency's attacks has migrated as new targets of opportunity presented themselves. When the coalition forces established a safe haven within the local environment, the insurgency procured missiles from Iran that were launched into the green zone (Washington Times 2007). When the country began to find its feet and stand up a police force, the insurgency murdered citizens as they stood in line to apply. The political races changed the landscape again, and presented new targets. Each time the community began to feel safe and establish routines, as reflected by the environment, the insurgency responded to the progress with creative devastation to prevent any long term stability.

Some innovations are indicative of the horizontal meme transfer pattern (Dove 2010b). Pulling from other fields, the insurgency has relied heavily upon the Internet for information exchange, transforming what began as an academic medium into a tool of war. To fund their efforts the insurgency has mimicked criminal enterprises the world over, "raising tens of millions of dollars a year from oil smuggling, kidnapping, counterfeiting, connivance by corrupt Islamic charities and other crimes that the Iraqi government and its American patrons have been largely unable to prevent" (Burns 2006). Their methods evolve as necessary to continue the fight employing innovations fueled by the foreign successes that are relayed virtually.

Harmonious Operation – General harmonious interaction between factions of the Iraqi Insurgency has prevailed. While consumed by the present threat of the coalition forces, they have set aside their differences to focus on the common foe. The "significantly differing ideologies that are currently cohesive based on a centralized threat of the US occupation" (Swanson 2007), override the historical distrust that pervades the culture. The insurgents have worked to capture the hearts of the population and are leveraging public expectations of corrupt government to promote their message of intolerance. Responding to public opinion, which should be regarded as an extended 'environment', individual groups "standardized their practices, resorting to those

deemed most legitimate and defensible pursuant to what Islamic jurisprudence calls the "ethics of jihad" (ICG 2006). In addition to securing their purpose in Islamic law, they have placed greater emphasis on establishing rapport among the community through compensation for loss and publicizing good deeds (ICG 2006). They are focusing on cultivating that environment of public opinion and allowing it to guide their actions.

Below are examples of how the insurgency employs both marker-based and sematectonic actions and responses, classified as either qualitative or quantitative.

The Insurgency makes extensive use of marker-based stigmergic communication. Qualitative stigmergy is apparent in the variety of websites that present distinct perspectives on the conflict and each encourages a specific behavioral response. The websites can be grouped into three categories:

- Those that portray resistance to occupation from a strict doctrinal point of view [mainstream Islamic websites], and scholars who explain meaning as presented in the Qur'an, the Sharia or the Hadith. Their impact on the worldwide Muslim community that provides moral and financial support to those fighting in Iraq is considerable (Adhami 2007).
- Those that portray the insurgent armed response to the occupation of Iraq as legitimate jihad (www.h-alali.net).
- Those that serve as the protected official communication channels for the insurgent groups fighting in Iraq. These sites "justify violence and indiscriminate attacks against 'enemies of Islam'" (Adhami 2007). They post videos of roadside bombings of US Military convoys, training of operatives, and skirmishes between coalition troops and the insurgents.

Each singular *jihadi* website that allows individual participants to deposit traces such as religious documents, graphic images, and individual postings is an example of quantitative marker-based stigmergy. The forums host intense indirect communication through forums where the agent may leave messages that influence the thinking and behavior of other agents around the world (Charette 2007). Much as a thread on a forum leads the reader along a trail, the page conveys its evolving message to the audience. The cumulative message incites others to act, which they do. Successful attacks, described in detail and glory, are disseminated to the masses via the website and unsurprisingly, are broadly emulated (ICG 2006).

Sematectonic stigmergic messages have been conveyed through intimidating acts in the physical environment. These include violent civilian killings, destruction of property and kidnappings with the intention of "intimidating, terrifying via a specific meaning: 'I'm willing to do this' and also 'I'm powerful and ready to act'" (Burbeck 2007). The acts accentuate the groups' divergent strategies, to include the nationalistic groups who use hostages for bartering and jihadists who use "filmed confessions and executions to prove their reach, power and intransigence" (ICG 2006). The brutality serves as stigmergic warnings, to some, while to others it conveys the weakness of the opposition and perceived 'puppet' government. The lack of security influences behavior of the population who, feeling frightened and vulnerable, do not participate in rebuilding efforts.

The type of violence committed is considered qualitative marker-based, and the perceived rate of violent acts, a quantitative marker-based stigmergic value. The 'environment' of any given

Provence is readily available via the media. The insurgents are "updating their beliefs and strategies based on the information and signals they receive from broadcast news, then deciding whether to execute an attack" (Johnson, 2009). The news coverage is a platform for stigmergic communication between insurgents, the population and the coalition. The broadcasting agent disperses a filtered perception of the environment, and the individual actors modify behavior accordingly (Robb 2009). For instance, news of a series of successful roadside bombings of military convoys might incline locals to avoid those routes, and alter traffic patterns.

IED Networks

Possibly considered a subset of the Iraqi Insurgency, the emergent network that develops and employs IEDs exhibits the characteristics of the adversarial stigmergic pattern. The pervasive use of IEDs has been declared "the single most deadly threat in Afghanistan" (SPAWAR 2010). By identifying the IED network as an agile system via the SAREPH characteristics, and defining its use of the adversarial stigmergic pattern, a step is taken toward understanding the threat, and developing methods to exploit that understanding.

Self-Organization – The highly organized network that is fundamental to the continued development and evolution of the IED is due to the self-organization of multiple entities, all contributing to the cause. Before a single explosive detonates, an entire informal supply chain comprised of "complex bodies of loose overlapping social partnerships" is engaged in the conception, design, development, and delivery of the device. This network of systems emerges from independent cells developing homemade weapons, intent upon confronting the occupying force. The attack itself leaves a stigmergic trace in the environment, acting as a signal to others that this is an effective means of being heard. Religious ideology, money, and social factors drive the fervent response to the signal, as ordinary people find their place in the web of systems that integrate to successfully develop, plant and detonate each IED (Swanson 2007).

Continued use of the IEDs changes the environment, from what was once a safe neighborhood where children played to one entrapped in war. The new landscape encourages the evolution of a network of systems, as individuals seek to contribute their skills to eliminating the foe, in response to what they observe. Each block of the network develops in response to a demand of the changing environment. Eventually, the system finances, recruits, indoctrinates/trains, safeguards, emplaces, and detonates, as well as develops, procures and assembles the IED, then identifies and prioritizes targets. The self-organized network is comprised of a fluid, linear decentralized structure, with modular architecture and sufficient redundancy to facilitate movement and change.

Adaptable Tactics – The IED developers' ever evolving efforts to disrupt the peacekeeping mission is the bane of the coalition forces. Once one deadly device is managed, another simple, inexpensive, lethal weapon appears on the battlefield efficiently retarding troop movement. The knowledge base of today's IED developers is the product of the "melting pot of global terrorism" (Higginbotham 2010), rooted in an infamous arms race that covered the same ground, but at a much slower pace. As "one of the most intensive and ingenious programs of homegrown bomb making R&D in history", Northern Ireland's Provisional IRA worked its way through every available bandwidth from model airplane controllers to cell phones (Higginbotham 2010). In an example of the horizontal meme transfer pattern (Dove 2010b), what took the IRA 30 years has shrunk to 18 months for the insurgency, due in no small part to the archival tenacity of the internet

environment. The lessons from innovations of another conflict have been resurrected, modified and successfully adapted. Additionally, each time the next solution was implemented, its effectiveness was clearly communicated—positively or negatively—via the media and populace, providing immediate stigmergic feedback to the nimble and eager manufacturer. The IEDs have evolved from early in the insurgency when they were often simple radio-controlled bombs to the latest weapon comprised of wood and no metal that is virtually undetectable, and positively lethal against coalition forces.

Reactive Resilience – When coalition forces counter an IED, such that it is no longer an effective tool, the mark is apparent in the environment as their freedom of movement increases. The IED network churns, operating at a reduced capacity until it successfully employs a new device, and again influences the environment. Likewise, when any aspect of the network is neutralized by the opponent, this too leaves a stigmergic trace of fewer IEDs being effectively employed. The network shifts in reaction to the loss, employing resources to adjust and recover, while the interim is marked by a diminished capacity to fight. In time the system evolves and recovers, leaving one trail abandoned and creating a new path to another source of the compromised component. At any time, when one link is eliminated the chain shifts and another takes its place.

Evolvable Strategies – As the IED networks established themselves and matured, the financial support landscape followed suit. Early in the conflict, when the system was emerging, insurgent efforts were funded by wealthy individuals from a distance. From the stigmergic perspective, money influenced target selection, and created a market for a new array of skills, thus shaping the environment. While unemployment soared, citizens stretched expertise and energetically applied themselves to this new income source. As the organization evolved, efforts became profit centric, diverging from ideology and more towards business endeavors. Success bread investment, ensuring that the networks, especially those sponsored by former regime elements, were well funded. Other sources such as, “national charities, private donors, mosques, ‘Zakat’ alms, and governmental organizations around the region are also contributors to insurgent groups” (Burns 2006). The additional income attracts skilled agents and generates interest in the operation, growing the network’s base.

Proactive Innovation – As long as there exists a perceived need to thwart coalition operations, IED developers have raised the creative bar to overcome each obstacle placed in their way. The Internet archives the stigmergic traces of those who have fought these battles previously, providing ready access to everything necessary to anticipate the opposition. Continuous evolution is easy when the creative tools and ideas of innovation are only a Google search away. The oracle’s wisdom has been called “The IED bazaar”, hosting device construction how-to manuals that illustrate assembly, deployment and detonation, in addition to an extensive video catalog of attacks (Grant 2010, Burns 2006).

The potent placement of IEDs, is influenced by the coalition’s movements within and use of the environment. For example, certain vehicles are suited to specific roadways, influencing the choice of effective IED to be employed in that area. Also, the proactive observation of movement and regular habits of troops, indicated by the marks they leave behind, influences the type, timing and placement of IEDs to the advantage of the insurgency.

Harmonious Operation – Identifying the explosive violence invoked by the IED network in harmony with its environment is outrageously counterintuitive. Yet, for the network to be so completely integrated into the society, such that it continues to execute successful operations in a climate inundated by coalition forces, points to a stigmergic harmony that leverages off signals and customs unfamiliar to the invaders. Built upon "adversarial groups operating in similar small autonomous adaptive cells that are independently orchestrated with no central authority and limited connection points", the network is integrated into the society, but does not behave as a normal social construct (ICG 2006). Each group remains intimate within themselves, minimizing outside contact but relying on strong connections to prior longstanding trusted contacts that remain dormant and undetectable until required and initiated.

The IED itself has blended in harmony with its surroundings. Laying in wait, the IED does not disrupt the environment, or call attention to its entombment. The explosive shape itself is invisible, the trigger undetectable, and scouts or triggermen blend naturally into the scene. The environment's stigmergic signals indicate to the wary convoy that all is well, it is safe to pass.

Below are examples of how marker-based and sematectonic actions and responses, classified as either qualitative or quantitative, are manifested.

Stigmergic signaling is a fundamental component of the IED network. The IED itself is clearly a marker-based stigmergic signal. In the discrete qualitative sense, the IED network employs various types of IEDs, each designed to target weaknesses in the opponent. As the opposition evolves and counters the IEDs, rendering them ineffective, the less-hostile environment is indicative of this change and the need for the network to innovate again. Similar to the quantitative stigmergic signaling within the insurgency itself, the IED network makes use of websites and forums to leave significant details of their experiences to induce action. Their postings are meant to guide other's work, flaunt success, and motivate their brethren in the struggle against the coalition forces.

Sematectonic stigmergy, where the modified environment elicits a response, is another aspect of communication within and to those outside of the IED network. The IED network modifies the environment in which coalition forces operate with each new IED that is successfully thwarted, or catastrophically discovered. The qualitative stigmergic act of introducing a modified IED to the environment adds another component of uncertainty and danger to the landscape, further advancing the agenda of the IED network. It forces change in the opposition, diverting resources to the stigmergic response to the new threat. Along the same lines, an example of quantitative sematectonic stigmergy is seen in the impact of multiple IED detonations upon a community. A significant increase or decrease in IED attacks changes the way a region is perceived. Additional activity draws those with skills in need of employment, and impels others to eschew the area completely. Behavior is based on the frequency and effectiveness of the IED incidents.

Cybercrime

The United States military, and militaries around the world, are standing up new commands that focus resources and their development to confront growing cyber security threats. The Internet pervades all aspects of life—in ways few truly understand—realizing societal vulnerabilities that have only been previously imagined in science fiction. In order to effectively counter the

increasing cyber criminal activity and protect our communities, the enemies must first be understood. Here we explore how the networks of cybercriminals operate as agile systems (per the SAREPH characteristics) and how their interactions reflect the stigmergic coordination pattern.

Self-Organization – Hacker networks exemplify the characteristics of a self-organizing emergent system using stigmergic communication as a rule. Hacker communities are dispersed geographically, forming on-line networks on forums that are loose open-structured entities. There they boast, share exploits, inspire ideas and engage in constructive discussion via forum postings indicative of marker-based stigmergy, fueling a highly innovative and constantly evolving decentralized network. Organization emerges on the forums, as leader-follower relationships develop, and individuals assume roles based on materializing needs. They remain fluid—if one agent's activity lapses another fills in—keeping members in line with the values they develop through virtual stigmergic interaction. The existence of these multi-national, virtual communities poses a threat to nation-states upon whom they are unleashing their fury (Still 2005).

Adaptable Tactics – Botnets, an autonomous collection of networked computers are the sledge hammers of the hacker's repertoire. Thousands of computers are enlisted to conjointly accomplish a task, usually nefarious in nature. Once established, the botnet can be rented out to perform denial of service attacks, or anything that requires the generation of a large volume of Internet traffic. Botnet communities often will have multiple command servers complete with controlling agents. In the past, the networks established a top down command and control infrastructure which was vulnerable to researchers and authorities who sought to identify and eliminate the key players (Fisher 2010). Adapting to the environment, the botnet community has morphed into more flexible and resilient peer-to-peer networks which allow the controllers essentially a world of options to choose from in the servers they employ (Fisher 2010). If a handful of servers is taken off line, others are used. This adaptation to the environment has made the entire operation of botnets significantly more robust and made the job of security experts much more difficult and time consuming, who accuse the botnet operators of monitoring their activities and adapting tactics over time to stay a step ahead of the game (Fisher 2010).

Reactive Resilience – The resilience of the hacker community refers to its ability to return to strength after a catastrophic reduction of capability, such as the elimination of a hacking network or defeat of a malware product. The established capability is diminished in either of these cases, but the motivating factors in the environment, be it money or ideology, persist, and those that were not destroyed inevitably seize the opportunity for themselves. When one botnet is thwarted, another is waiting to be employed to accomplish the task in a more robust manner, having learned from the destruction of its peer. If one network of hackers is identified and shut down, it reemerge as a new face, under a different avatar, and reestablish the pursuit. As long as the Internet remains integrated into every aspect of our civil structure, from power grids, to traffic lighting, banking, and corporate communication, and is inadequately protected, the environment is ripe for reemergence of new methods attacking new vulnerabilities—the bait is too tantalizing to resist.

Evolvable Strategies – The Internet and cyber capability have been integrated into our experience from their origins in academia to Internet banking, e-commerce, and the social networking of face book, forming an ever changing environment that continually presents new opportunity for cyber crime. Transgressions have evolved from exploiting the unsecured and unsuspecting, to

threatening nation-state economic foundations. A book called "Unrestricted Warfare" was published in China in 1999 advocating not engaging the U.S. directly, but "understanding and employing the principle of asymmetry correctly to allow us [the Chinese] always to find and exploit an enemy's soft spots" (SPAWAR 2010). These indirect attacks are very real as computer hackers from multiple countries have penetrated deeply into the information systems of U.S. companies and government. In April 2001, Chinese hackers reportedly destroyed large volumes of data on the US Web servers they attacked in the aftermath of the EP-3 crisis (Krekel 2009). From the stigmergic perspective, as the cyber environment took on additional dimensions (the environment changed), cyber criminal strategies and behavior have rapidly evolved to be the first to capitalize upon unchartered territory.

Proactive Innovation – Cyber criminals employ proactive innovation regularly to defeat the next generation of cyber security defenses. Internet forums provide opportunities for cross communication between hackers dedicated to disparate causes, and become a petri dish of idea exchange. One group draws upon the experiences of others to innovate their way over obstacles and morph their responses to a changed environment. When a software vulnerability is closed hackers easily go to their sources and purchase information on another software security hole and go about new exploitations. As discussed previously, hackers have noted that botnets are compromised in time, and innovated operational modifications that have recently made complete elimination of a given botnet virtually impossible.

Harmonious Operation – The Internet is integral to our experience, and no longer foreign to our environment. Remote operation of most anything utilizes some aspect of cyberspace. It has become ubiquitous and we have adapted, now expecting the convenience of control and information that is only a click away. Parasitic cybercrime too silently blends in with emails and websites, striking suddenly and covertly, often without detection. The response of the populace to cyber crime is lethargic—most don't understand how to operate their computers effectively, let alone protect themselves from the lurking dangers that seem nowhere, but may be everywhere.

Below are examples of how both marker-based and sematectonic actions and responses, classified as either qualitative or quantitative, are manifested .

Cybercrime is stigmergic in that its products (viruses, malware etc.) are traces left in the Internet operating environment that invoke behavior shifts in agent perpetrators. Each new piece of malware is qualitative marker-based stigmergy that signals recruits a growing number of employers. Successful malware leads an agent down a specific path, just as a pheromone leads an ant to food. Quantitative marker-based stigmergy is occurs when the media makes it known that a particular type of attack is amassing great success, and the effect is amplified as more employers of the attack are recruited due to its evident success.

Considering cybercrime from a broader perspective, the sematectonic stigmergic responses to the altered environment become apparent. As criminal behavior via the Internet became prevalent, threatening, then invading the operations of the nation-state, governments acted to protect their interests. Cyber security centers and commands were created, and funding was identified to supply resources to fight the enemy. As the shape of the environment changes, a change in behavior of the perpetrating agents emerges. Sematectonic stigmergy occurs as the environment changes and

signals new response mechanisms. The success of Wikileaks now being mimicked by alternative but similar paths is an example of quantitative sematectonic stigmergy. Stuxnet is now feared as a possible example of qualitative sematectonic stigmergy, expected to ring in a new level of weaponized cyber attack. As new aspects of an Internet connected infrastructure mature, the scene assumes an altered form that entices new experiments and new paths.

Conclusions and Direction for Further Work

Human-human stigmergic communication is ubiquitous in society, influencing the daily behavior of our peers and adversaries. Each of the notable adversaries considered in this study, the Iraqi Insurgency, IED Networks, and Cybercriminals, rely heavily upon traces left in the environment for indirect communication. They read the stigmergic signals to determine how to most effectively employ and improve their weapon of choice. The opponent's agile networks manipulates the environment to control their enemy via indirect means.

In understanding the stigmergic interactions of our adversary we make progress toward developing effective agile security strategies that are capable of sparing with that evolving and resourceful foe. The definition of the stigmergic interaction pattern and exploration of the SAREPH characteristics for both academic examples and notable adversaries is another step toward facilitating communication between the key players in security systems development. By examining high profile adversaries in light of the new pattern and identifying key examples that will be relevant and familiar to an array of backgrounds, this effort contributes new tools to the pattern project. We expect that the research started here will enable systems engineers, security engineers and decision makers to better understand and communicate the enemy's methodology, and in so understanding, develop agile security systems that guarantee the integrity of our boarders and our freedoms.

The process of framing the selected adversarial system within the context of the stigmergic interaction pattern emphasized the connection of the agent with the environment, and suggests opportunities to better understand intervention strategies to disrupt effectiveness. The pattern evokes the significance of the agent's perception of the environment, which was demonstrated across the systems examined. If the agent doesn't perceive an opportunity to evolve—if the environment doesn't present a new face—the agent is stagnant. Likewise, if the ability to place markers is eliminated—or the interpretation of those markers is filtered—the system is at a loss for communication. Considering the adversary through the stigmergic pattern framework identifies potential vulnerabilities and opportunities to work toward effective exploitation.

Continuing pattern work will take into account the statistical action and response core of stigmergy, and expand the understanding and use of the stigmergic pattern by developing means for eliminating or manipulating communication via the environmental medium.

References

1. Adhami, W. 2007. The strategic importance of the Internet for armed insurgent groups in modern warfare, *International Review of the Red Cross* Vol 89, No. 868, Dec.
2. Beckers, R., O. E. Holland, and J. L. Deneubourg. 1994. "From Local Actions to Global Tasks: Stigmergy and Collective Robotics." In In R. Brooks & P. Maes (Eds.), Artificial life IV (pp. 181-189. Cambridge, MA (US): MIT Press.
3. Burbeck, Steve. 2007. Complexity and the Evolution of Computing: Biological Principles for

Managing Evolving Systems. V2.2, May. On lIne and available 03Nov2011 at http://evolutionofcomputing.org/Complexity%20and%20Evolution%20of%20Computing%20v2.pdf
4. Burns, John F. and Kirk Semple. 2006. U.S. Finds Iraq Insurgency Has Funds to Sustain Itself. The New York Times, 26 Nov.
5. Charette, R. N. 2007. Blog:Open-Source Warfare: Terrorists are leveraging information technology to organize, recruit, and learn—and the West is struggling to keep up. IEEE Spectrum, November. http://spectrum.ieee.org/telecom/security/opensource-warfare
6. Dove, Rick and Laura Shirey. 2010a. On Discovery and Display of Agile Security Patterns, Conference on System Engineering Research, Hoboken, NJ, March 17-19.
7. Dove, R. 2010b. Pattern Qualifications and examples of Next-Generation Agile System-Security Strategies, IEEE International Carnahan Conference on Security Technology (ICCST), San Jose, CA, USA, 5-8 Oct. www.parshift.com/Files/PsiDocs/PatternQualificationsForAgileSecurity.pdf
8. Dreazen, Yochi J. 2010. Using Drones to Counter IEDs, A military task force tries a new method against bombers in Afghanistan, National Journal Magazine, 2 Oct.
9. Elliott, Mark. 2006. Stigmergic Collaboration: The Evolution of Group Work. M/C Journal 9.2.
10. Fisher, D. 2010. Botnets Using Ubiquity as Security. *The Kaspersky Lab Security News Service*, 7 Jun. http://threatpost.com
11. Grant, G. 2010. Afghan IEDs Show Rapid Adaptation, *DoD Buzz Online Defense and Acquisition Journal*, 12 Apr. www.dodbuzz.com/2010/04/12/afghan-ieds-show-accelerated-adaptation/?wh=wh#axzz0l0Bauhhp (accessed 26 Sep 10)
12. Heylighen F. 2007. Accelerating Socio-Technological Evolution: from ephemeralization and stigmergy to the global brain, In: Globalization as an Evolutionary Process: Modeling Global Change, edited by George Modelski, Tessaleno Devezas, and William Thompson, London: Routledge, p.286-335.
13. Higginbotham, A.. 2010. U.S. Military Learns to Fight Deadliest Weapons. *Wired*. Aug.
14. International Crisis Group. 2006. *In Their Own Words: Reading the Iraqi Insurgency*. International Crisis Group Middle East Report 5, 15 Feb. Brussels, Belgium.
15. Johnson, N., 2009 "Common Ecology quantifies human insurgency", Nature 462, 911-914
16. Krekel, Bryan . 2009. Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. prepared for The US-China Economic and Security Review Commission, Northrop Grumman. pp 68-69.
17. Parunak, H. V. 2003. Making Swarming Happen. In Proceedings of Swarming: Network Enabled C4ISR. Tysons Corner, VA, 3 Jan. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.116.1990&rep=rep1&type=pdf
18. Parunak, H. V. A. 2005a. Expert Assessment of Human-Human Stigmergy. Analysis for the Canadian Defence Organization, Altarum Institute, Ann Arbor, MI,October. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA440006&Location=U2&doc=GetTRDoc.pdf
19. Parunak, H. V. A.. 2005b. Survey of Environments and Mechanisms for Human-Human Stigmergy. In proceedings Environments for Multi-Agent Systems II: Second International Workshop, E4MAS 2005, Utrecht, The Netherlands, July 25. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.6974&rep=rep1&type=pdf
20. Robb, J. 2007. *Brave New War*, John Wiley & Sons, Inc., Hoboken, NJ. p 116-117.

21. Robb, J. 2009 JOURNAL: A Critique of Open Source Warfare, *Global Guerrillas (Blog)* http://globalguerrillas.typepad.com/http://globalguerrillas.typepad.com/globalguerrillas/2009/12/journal-a-critique-of-open-source-warfare.html
22. SPAWAR (Space and Naval Warfare Systems Center Atlantic). 2010, An Overview of the Cyber Warfare, Exploitation & Information Dominance (CWEID) Lab. Presented to the CDCA Small Business & Industry Outreach Initiative Symposium. Vincent Van Houten, SGLC, IA Engineering & Cyber Defense Division, 58200. 28 Jan.
23. Still, Brian. 2005. Hacking for a Cause. First Monday. Volume 10, Number 9. http://firstmonday.org/issues/issue10_9/still/index.html
24. Swanson, S. 2007, Viral targeting of the IED Social Network System. *Small Wars Journal* Vol 8, May.
25. Tapper, J. 2006. Iraqi Insurgents Increasingly Using Internet as Propaganda Machine. *ABC News*, 14 Feb. http://abcnews.go.com
26. Washington Times. 2007. Iran arms Iraqi insurgents The Washington Times. February 12.

Biography

Jena Lugosky orchestrates the modification and integration of combat ready systems to the Naval war fighter as a Project Engineer at L3 Communications/Platform Integration Systems. She served as an officer in the United States Air Force and holds a Bachelor of Science in Mechanical Engineering from Rensselaer Polytechnic Institute and a Master of Science in Physics from Louisiana Tech University. She is currently completing a Masters of Engineering in Systems Engineering through Stevens Institute of Technology.

Rick Dove develops agile self-organizing systems as a principle investigator and application program manager at Paradigm Shift International, and chairs the INCOSE working group for Systems Security Engineering. He is an adjunct professor at Stevens Institute of Technology in the School of Systems and Enterprises, and author of Response Ability – the Language, Structure, and Culture of the Agile Enterprise. He co-led the OSD/Navy-funded project that identified systems agility as the new competitive factor, and then led the research at the DARPA/NSF-funded Agility Forum. He holds a BSEE from Carnegie Mellon University, with graduate work in Computer Science at U.C. Berkeley.