Journal of Strategic Security

Volume 8
Number 3 *Volume 8, No. 3, Special Issue Fall 2015: Intelligence: Analysis, Tradecraft, Training, Education, and Practical Application*

Article 7

The Cyber Intelligence Challenge of Asyngnotic Networks

Edward M. Roche
Columbia Institute for Tele-Information, Columbia University, emr96@columbia.edu

Michael J. Blaine

John McCreary
Defense Intelligence Agency (ret.)

Recommended Citation
Roche, Edward M.; Blaine, Michael J.; and McCreary, John. "The Cyber Intelligence Challenge of Asyngnotic Networks." *Journal of Strategic Security* 8, no. 3 (2015) : 107-136.
DOI: http://dx.doi.org/10.5038/1944-0472.8.3.1448
Available at: https://scholarcommons.usf.edu/jss/vol8/iss3/7

The Cyber Intelligence Challenge of Asyngnotic Networks

Author Biography

Edward M Roche, Ph.D., J.D. is a member of the California Bar. Michael J Blaine holds an MBA in finance from New York University and a Ph.D. in international business from Ohio State University. John McCreary is publisher of the daily Night Watch intelligence briefing and a retiree from the Defense Intelligence Agency.

Abstract

The intelligence community is facing a new type of organization, one enabled by the world's information and communications infrastructure. These asyngnotic networks operate without leadership and are self-organizing in nature. They pose a threat to national security because they are difficult to detect in time for intelligence to provide adequate warning. Social network analysis and link analysis are important tools but can be supplemented by application of neuroscience principles to understand the forces that drive asyngnotic self-organization and triggering of terrorist events. Applying Living Systems Theory (LST) to a terrorist attack provides a useful framework to identify hidden asyngnotic networks. There is some antecedent work in propaganda analysis that may help uncover hidden asyngnotic networks, but computerized SIGINT methods face a number of challenges.

Introduction

In June of 2014, someone leaked to the press that the infamous computer hacking group, Anonymous, was preparing to start operation NO2ISIS to strike against supporters of the Islamic State of Syria and al-Sham (ISIS).[1] The anonymous source stated:

> "We plan on sending a straightforward message to Turkey, Saudi Arabia, Qatar and all other countries that evidently supply ISIS for their own gain," the source said. "In the next few days we will begin defacing the government websites of these countries so that they understand this message clearly. We are unable to target ISIS because they predominately fight on the ground. But we can go after the people or states who fund them."[2]

One of the motivating factors behind this attack appears to be that the Twitter feed @theanonmessage had been taken over by ISIS and used to distribute graphic images of violence. On January 22, 2015, it was reported that the Anonymous "Red Cult Team" had taken down ISIS websites in response to the murder of the Charlie Hebdo journalists in Paris. An Anonymous twitter feed @OpCharlieHebdo confirmed that the website ansar-alhaqq.net had been "taken down,"[3] as well as other ISIS websites.[4]

This faceless cyber-war quickly escalated. By February 8, 2015, Anonymous[5] reported that it had taken control of "dozens of Twitter and Facebook

[1] Hamill, J., "Anonymous hacktivists prepare for strike against ISIS 'supporters,'" (2014) *Forbes*, available at: *http://www.forbes.com/sites/jasperhamill/2014/06/27/anonymous-hacktivists-prepare-for-strike-against-isis-supporters/*.

[2] A full text of the Anonymous statement is at the end of this paper.

[3] Vandita, 2015a, Anonymous takes down ISIS websites, confirms leaked government documents were real, *We Are Anonymous* website, available at: *http://www.anonhq.com*.

[4] The list was included in a number of tweets: "#Target joinalqarda.com 144.76.97.176 #TANGODOWN; #Target alintibana.net 144.76.97.176 #TANGODOWN; #Target opcharliehebdo.com 104.28.7.87 (Imposter Website)#TANGODOWN; #Target islaam.com 97.74.45.128 #TANGODOWN; #Target Qa3edon.100free.com 205.134.165.186 #TANGODOWN; #Target daulahisamiyah.net 119.81.24.187 #TANGODOWN; #Target ansar1.info 79.172.193.108 #TANGODOWN; and #Target jhuf.net 104.28.20.19 #TAN- GODOWN". *Note:* The term "#TANGODOWN" is Anonymous reporting that the site had been taken down. One assumes that "tango" is the call sign for the letter "T" abbreviating "taken".

[5] Anonymous is a loosely associated international network of activist and hacktivist entities. It does not have a leadership structure.

accounts" that had been used by ISIS to spread their influence through social media.[6] Anonymous released a video on YouTube openly threatening ISIS:

> "We will hunt you, take down your sites, accounts, emails, and expose you. From now on, no safe place for you online . . . You will be treated like a virus, and we are the cure . . . We own the Internet . . . We are Anonymous; we are Legion; we do not forgive, we do not forget, Expect us."[7]

It then identified 90 twitter accounts and 12 Facebook accounts that "appear to be in close contact with ISIS". Shortly after this information was released, both Twitter and Facebook took down the accounts. If this had been a kinetic war, these actions would have been equivalent to severely degrading command and control by taking out a major telecommunications center.

Only a few days later, February 19th, 2015, Anonymous reported that its #OpISIS operation was in "Round 2" and had "exposed *thousands* of ISIS accounts to show that it is not that difficult to fight back against ISIS online"[8] (emphasis added). It also provided a list of 3,030 accounts that it had handed over to Twitter with the message "do your job" [and suspend the accounts].[9] Anonymous then released a video stating that its actions were "to show what your governments are *not* doing" (emphasis added). By February 25, it was reporting on "#OpISIS Round 4" with the headline "Anonymous Beats United States in Combating Terrorism". Then in a stunning move, it released for anyone wishing to view it, a list containing the contact information, IDs, usernames, passwords and other information for all members of a leading ISIS website.[10]

[6] CoNN, 2015. Anonymous "hacktivists" strike a blow against ISIS. We Are Anonymous website www.anonhq.com; Blair, L., 2015. Anonymous says ISIS is not Muslim, hacks hundreds of ISIS accounts online; says 'we are Muslims, we are Christians'. *The Christian Post* , np.

[7] Anonymous, 2015. Anonymous #OpISIS continues. YouTube video posting.

[8] Vandita, 2015b. #OpISIs Round 2: Anonymous hacks thousands of ISIS accounts. We Are Anonymous website www.anonhq.com.

[9] David, Z., 2015. Anonymous hacks more ISIS accounts than ever, after U.S. government and Twitter refuse to act. *Counter Current News* , np.

[10] You can view the list at: http://http://pastebin.com/rbq8s4GM. The data included "id", "username", "password", "category", "name", "timeslogin", "refered", "credits", "sizedownloaded", "expirydate", "registrationdate" for a large number of accounts. *See* Team, A.R.C., 2015, #OpISIS – database hacked by Anonymous Red Cult Team. Pastebin.com.

It appears that the #OpISIS operation conducted by Anonymous was a success. These operations were conducted with a large amount of technical skill, and have been timely. But who is doing the work? Who is Anonymous? How is it organized, and are there other groups operating in the same way? Can such an organization wage a cyber war more effectively than the world's nation-states? Has it been more effective than the U.S. Cyber Command or its counterpart in other countries?[11]?

This paper argues that the intelligence community is facing a new type of organization, one enabled by the world's information and communications infrastructure, and not having the traditional characteristics of any organization known before. These networks of persons operate without leadership. They communicate using both controlled and open un-controlled paths for handling information, and they organize themselves in an unconscious (un-planned) way. They are self-organizing networks. What is peculiar is that these networks, such as Anonymous, appear to be highly effective, but do not share any of the characteristics of a typical organization.[12] That is, the individual components of a legacy terrorist network such as an identifiable leadership structure for command and control is not present.

Apart from Anonymous, we can see this type of organization in other places as well. It is present in broad social movements such as Occupy Wall Street, the Arab Spring, Internet policy coalitions, and anti-globalization drives. It is apparent in ISIS recruiting through social media, where we see what appear to be random youth in developed Western countries give up their entire life and manner of living to join the caliphate and its uncertain future.[13] No one yet fully understands how these convincing communications take place and why unexpected recruits from around the world are joining the caliphate to fight, even without explicit orders. This is because the ISIS phenomenon is working in the same self-organizing way.[14]

[11] The United States Cyber Command (USCYBERCOM) is an armed forces sub-unified command subordinate to the United States Strategic Command. It is located in Fort Meade, Maryland at NSA.

[12] See the related discussion in Cetina (2005) who writes about "microstructures" forming networks.

[13] The ISIS phenomenon outside of Iraq and Syria is operating in an asyngnotic way; but at home, ISIS is operating with a typical organizational form.

[14] ISIS as an organization operating in Iraq and Syria has a classical organizational form, e.g., a leader, assistants, functional specialization, command and control. It is the wider ISIS phenomenon that is characterized by asyngnosis and asyngnotic behavior.

In order to examine this type of shadowy organization, we propose a simple framework that we call 'Asyngnosis'. The word is constructed from Greek: α- (not) + συνειδιτος- (conscious) + γνοσι- (knowledge, information); and describes the undirected emergence of knowledge and other interconnected pathways that form around a specific idea or activity. We would argue that an 'Asyngnodic' (+ δικτυο - grid or network) (an asyngnotic network) may describe many complex organizational activities, particularly decision-making and operations. Decisions and strategies may be modeled as not the outcome of a complex, structured set of discrete activities or processes, but instead as the product of continuous (non-discrete) flows of information, ideas and impressions ('memes')[15] along ever-changing communication pathways tying together individuals and organizations. Much like the pathways between neurons in the brain, these networks are characterized by their constant formation, strengthening, weakening, and disappearance based on use and need, yet as these connections and disconnections take place, the organization itself constantly changes.[16]

Both the continuous flow of memes and the constant reconfiguration of these networks takes place not only between individuals, but between individuals and organizations, and between the organizations themselves without regard to national, cultural, or even linguistic boundaries. Thus, in its simplest form, Asyngnosis combines four concepts: a) memes (information, concepts, impressions); b) a continuous nature (non-discrete events); c) networks (communication paths; influence paths; sensory paths); d) plasticity (spontaneous reconfigurablity) and *ad hoc* formation and dissolution).

In the remainder of this article, we will review several approaches used in intelligence to analyze networks of criminals, terrorists or other persons or organizations who threaten national security. We will show that these techniques, although powerful, fail to address the specific challenges of the asyngnotic form of network. Next, we will discuss the nature of asyngnotic behavior. After that, we will present a short example of how an asyngnotic network approach could be used to understand the *Charlie Hebdo* terrorist attack in Paris. Here we use a parallel in Living Systems Theory (LST) to make an initial identification of unseen networks. LST is reviewed briefly in the appendix.

[15] Ferguson (Ferguson, N., "Networks and hierarchies," *The American Interest* (2014) 9, 16–24) also mentions memes.

[16] To see this pattern in the activities of Anonymous or other hacker groups, it is only necessary to examine the shifting pattern of content over the years.

We will then discuss the intelligence challenges for automated collection and analysis of intelligence data needed to anticipate this type of event. Much of our approach is based on neuroscience, because some of its underlying theory regarding the brain, including quantitative measurements of action potentials, might be used to model the information flow and SIGINT characteristics of self-learning leaderless networks.

Current Intelligence Approaches

Theory of Social Networks

The analysis of social networks has a rich history starting with the work of Ëmile Durkheim, considered to be the father of sociology. Some of the earliest work in diagramming and network analysis focused on derivation of a social structure. It was considered that "the dynamic meaning of chain-relations in social structure is better understood in view of a network hypothesis."[17] Early studies examined how information is passed through social networks[18] and these models also were useful for understanding diffusion of innovation, spread of a disease, cognitive social structures,[19] the abstract idea of social capital,[20] and even sexual behavior.[21] Study of the strength of ties between persons was found to influence how well a message could be propagated (wider propagation with *weaker* ties).[22] Over time, these methods became computerized, and the rise of social network analysis may have come with the rise of social media.

Analysis of Social Media

The rapid growth of social media has provided an important platform for social network analysis, because an adequate amount of information is available openly online. These giant social networks are easy to view because

[17] Moreno, J.L., Jennings, H.H., "Statistics of social configurations," *Sociometry* (1938) 1, pp. 342–374. These first social networks are literally hand-drawn in the journals, very different from today's outputs from computerized mapping software.

[18] Rapoport, A., "Spread of information through a population with socio- structural bias: I. assumption of transitivity," *The Bulletin of Mathematical Biophysics* (1953) 15, 523–533; Rapoport, A., "A study of a large sociogram*," Behavioral Science* (1961) 6, 279–291.

[19] Krackhardt, D., "Cognitive social structures," *Social Networks* (1987) 9, 109 – 134.

[20] Burt, R.S., "The contingent value of social capital," *Administrative Science Quarterly* (1997) 42, 339.

[21] Laumann, E.O., "A 45-year retrospective on doing networks," *Connections* (2006) 27, 65–90.

[22] Granovetter, M.S., "The strength of weak ties," *American Journal of Sociology* (1973) 78, 1360–1380.

automation can be used to collect massive amounts of data. Indeed, social networks such as Facebook, Google+, or LinkedIn have publicly visible data that reveals every "friend" a person is connected to as well as a record of their interactions and indicators of similarity. Using this information, it is possible automatically to data-mine social networks and correlate the derived network structure surrounding an individual or group with other known information describing the participating individuals, e.g., preferences, location, sex, etcetera. For example, many have studied how social media can be used by businesses to develop next generation products[23] or assess whether a product is appropriate to sell online[24]. Other applications include customer relationship management,[25] identification of promising investments,[26] and identification of stakeholder groups that may influence corporate policy.[27] Because of its effect on how consumers purchase online,[28] much work has been done on recommendation systems,[29] word-of-mouth evaluations,[30]

[23] Li, Y.M., Chen, H.M., Liou, J.H., Lin, L.F., "Creating social intelligence for product portfolio design," *Decision Support Systems* (2014) 66, 123 – 134; Lau, R.Y., Li, C., Liao, S.S., "Social analytics: Learning fuzzy product ontologies for aspect-oriented sentiment analysis," *Decision Support Systems* (2014) 65, 80 – 94. Crowdsourcing and Social Networks Analysis.

[24] Verbraken, T., Goethals, F., Verbeke, W., Baesens, B., "Predicting online channel acceptance with social network data," *Decision Support Systems* 63 (2014) 104 – 114. 1. Business Applications of Web of Things 2. Social Media Use in Decision Making.

[25] van Dam, J.W., van de Velden, M., "Online profiling and clustering of Facebook users," *Decision Support Systems* (2015) 70, 60 – 72.

[26] Gottschlich, J., Hinz, O., "A decision support system for stock investment recommendations using collective wisdom," *Decision Support Systems* (2014) 59, 52 – 62.

[27] Jiang, S., Chen, H., Nunamaker, J.F., Zimbra, D., "Analyzing firm-specific social media and market: A stakeholder-based event analysis framework," *Decision Support Systems* (2014) 67, 30 – 39.

[28] Gao, J., Zhang, C., Wang, K., Ba, S., "Understanding online purchase decision making: The effects of unconscious thought, information quality, and information quantity," *Decision Support Systems* (2012) 53, 772 – 781. 1) Computational Approaches to Subjectivity and Sentiment Analysis 2) Service Science in Information Systems Research : Special Issue on {PACIS} 2010.

[29] Li, X., Wang, M., Liang, T.P., "A multi-theoretical kernel-based approach to social network-based recommendation," *Decision Support Systems* (2014) 65, 95 – 104. Crowdsourcing and Social Networks Analysis.; Geiger, D., Schader, M., "Personalized task recommendation in crowdsourcing information systems — current state of the art," *Decision Support Systems* (2014) 65, 3 – 16. Crowdsourcing and Social Networks Analysis.; Liao, H.Y., Chen, K.Y., Liu, D.R., "Virtual friend recommendations in virtual worlds," *Decision Support Systems* (2015) 69, 59 – 69.

[30] Zhang, Z., Li, Q., Zeng, D., Gao, H., "User community discovery from multi-relational networks," *Decision Support Systems (*2013) 54, 870 – 879.; Chang, H.H., Tsai, Y.C., Wong, K.H., Wang, J.W., Cho, F.J., "The effects of response strategies and severity of failure on consumer attribution with regard to negative word-of-mouth," *Decision Support Systems* (2015) 71, 48 – 6.; Bao, T., Chang, T.L., "Finding disseminators via electronic word of mouth message for effective marketing communications," *Decision*

product reviews,[31] and the effects of social media on the reputation of a business[32] or public opinion in general.[33] Some work has attempted to explore social media as a prediction market.[34]

Much of this work is done using text mining to uncover information about social media users.[35] It has been recognized that social media may have a strong effect on the behavior of individuals. Some have explored non-conscious intentions,[36] why people keep coming back to social media,[37] psychological addiction,[38] and maladaptive cognition.[39] Individuals exhibit

Support Systems (2014) 67, 21 – 29.; Cheung, C.M., Thadani, D.R., “The impact of electronic word-of-mouth communication: A literature analysis and integrative model,” *Decision Support Systems* (2012) 54, 461 – 470.

[31] Bao, T., Chang, T.L., “Finding disseminators via electronic word of mouth message for effective marketing communications,” *Decision Support Systems* (2014a) 67, 21 – 29.; Yu, H., Shen, Z., Miao, C., An, B., Leung, C., “Filtering trust opinions through reinforcement learning,” *Decision Support Systems* (2014) 66, 102 – 113.; Ku, Y.C., Wei, C.P., Hsiao, H.W., “To whom should I listen? Finding Reputable Reviewers in Opinion-sharing Communities,” *Decision Support Systems* (2012) 53, 534 – 542.

[32] Vavilis, S., Petkovi ´c, M., Zannone, N., “A Reference Model for Reputation Systems,” *Decision Support Systems* (2014) 61, 147 – 154.; Schniederjans, D., Cao, E.S., Schniederjans, M., “Enhancing Financial Performance with Social Media: An Impression Management Perspective,” *Decision Support Systems* (2013) 55, 911 – 918. 1. Social Media Research and Applications 2. Theory and Applications of Social Networks.; da Silva, N.F., Hruschka, E.R., Jr., E.R.H., “Tweet Sentiment Analysis with Classifier Ensembles,” *Decision Support Systems* (2014) 66, 170 – 179.

[33] Tian, R.Y., Liu, Y.J., “Isolation, Insertion, and Reconstruction: Three Strategies to Intervene in Rumor Spread Based on Supernetwork Model,” *Decision Support Systems* (2014) 67, 121 – 130.

[34] Qiu, L., Rui, H., Whinston, A., “Social Network-Embedded Prediction Markets: The Effects of Information acquisition and communication on predictions,” *Decision Support Systems* (2013) 55, 978 – 987. 1. Social Media Research and Applications 2. Theory and Applications of Social Networks.

[35] Lu, H.M., “Detecting short-term cyclical topic dynamics in the user- generated content and news,” *Decision Support Systems* (2015) 70, 1 – 14.

[36] Zhao, K., Stylianou, A.C., Zheng, Y., “Predicting users’ continuance intention in virtual communities: The dual intention-formation processes,” *Decision Support Systems,* (2013) 55, 903 – 910. 1. Social Media Research and Applications 2. Theory and Applications of Social Networks.

[37] Gwebu, K.L., Wang, J., Guo, L., “Continued usage intention of multi- functional friend networking services: A test of a dual-process model using Facebook,” *Decision Support Systems* (2014) 67, 66 – 77.; Al-Debei, M.M., Al-Lozi, E., Papazafeiropoulou, A., “Why people keep coming back to Facebook: Explaining and predicting continuance participation from an extended theory of planned behavior perspective*,” Decision Support Systems* (2013) 55, 43 – 54.; Sun, Y., Fang, Y., Lim, K.H., “Understanding sustained participation in transactional virtual communities,” *Decision Support Systems* (2012) 53, 12 – 22; Cheung, C.M., Lee, M.K., “A theoretical model of intentional social action in online social networks,” *Decision Support Systems* (2010) 49, 24 – 30.

[38] Wang, C., Lee, M.K., Hua, Z., “A theory of social media dependence: Evidence from microblog users,” *Decision Support Systems* (2015) 69, 40 – 49.

[39] *Ibid.*

different leadership styles in online communities,[40] they disclose probably too much information about themselves,[41] and use different habits in making decisions.[42] Content analysis can be used to discover a variety of social roles assumed online.[43] Some work has used automated tools to examine the effects and operations of social networks including allocation of workflows,[44] span of control as a function of trust,[45] and the functions of online support communities.[46]

Finally, a significant amount of work has been done in developing automated tools for exploration of the structure of social networks. Zhang[47] used author-topic data to derive multi-relational networks in social media, and Zhou[48] showed it is possible to discover *implicit* social networks. Han[49] was able to mine Facebook data and uncover individual preferences and interests. Other work in data mining[50] has focused on identification of friendships,[51] inferences of shared interests between individuals,[52] identification of gatekeepers and subgroups,[53] organizational structure[54] and knowledge

[40] Templeton, G.F., Luo, X.R., Giberson, T.R., Campbell, N., "Leader personal influences on membership decisions in moderated online social networking groups," *Decision Support Systems* (2012) 54, 655 – 664.

[41] Chen, R., "Living a private life in public social networks: An exploration of member self-disclosure," *Decision Support Systems* (2013) 55, 661 – 668.

[42] Sadovykh, V., Sundaram, D., Piramuthu, S., "Do online social networks support decision-making?" *Decision Support Systems* (2015) 70, 15 – 30

[43] Lee, A.J., Yang, F.C., Tsai, H.C., Lai, Y.Y., "Discovering content-based behavioral roles in social networks," *Decision Support Systems*, (2014) 59, 250 – 261.

[44] Bajaj, A., Russell, R., "Awsm: Allocation of workflows utilizing social network metrics," *Decision Support Systems* (2010) 50, 191 – 202.

[45] Salas-Fumás, V., Sanchez-Asin, J.J., "Information and trust in hierarchies," *Decision Support Systems* (2013) 55, 988 – 999. 1. Social Media Research and Applications 2. Theory and Applications of Social Networks.

[46] Sutanto, J., Kankanhalli, A., Tan, B.C., "Uncovering the relationship between user support networks and popularity," *Decision Support Systems,* (2014) 64, 142 – 151

[47] Zhang, Z., Li, Q., Zeng, D., Gao, H., "User community discovery from multi-relational networks," *Decision Support Systems* (2013) 54, 870 – 879.

[48] Zhou, W., Duan, W., Piramuthu, S., "A social network matrix for implicit and explicit social network plates," *Decision Support Systems* (2014) 68, 89 – 97.

[49] Han, X., Wang, L., Crespi, N., Park, S., Cuevas, A., "Alike people, alike interests? Inferring interest similarity in online social networks," (2015) *Decision Support Systems* 69, 92 – 106.

[50] Chen, Y.L., Wu, Y.Y., Chang, R.I., "From data to global generalized knowledge," *Decision Support Systems* (2012) 52, 295 – 307.

[51] Liao, H.Y., Chen, K.Y., Liu, D.R., "Virtual friend recommendations in virtual worlds," *Decision Support Systems* (2015) 69, 59 – 69

[52] Han, X., Wang, L., Crespi, N., Park, S., Cuevas, A., "Alike people, alike interests? Inferring interest similarity in online social networks," *Decision Support Systems* (2015) 69, 92 – 106.

[53] Zhu, B., Watts, S., Chen, H., "Visualizing social network concepts," *Decision Support Systems* (2010) 49, 151 – 161.

flows.[55] Although these techniques of analysis at first were developed in the commercial sector, particularly advertising, some of the underlying methodologies have turned out to be useful frameworks for intelligence, but using an extended data set based on SIGINT.

Application of Network Analysis – Link Analysis and Complex Correlation

As a type of applied social network theory, link analysis has been widely exploited in intelligence analysis.[56] Although earlier intelligence work was done manually,[57] in criminal intelligence, the concept of network centrality has be used to identify vulnerabilities in criminal organization,[58] identify false identities,[59] and find hidden networks and web communities.[60] Link analysis using a variety of attributes of hate group web sites has been used to map affiliations between different groups of radicals,[61] guerrillas[62] and terrorists.[63] There are important applications in combatting identity theft.[64] There are

[54] Qiu, J., Lin, Z., "A framework for exploring organizational structure in dynamic social networks," *Decision Support Systems* (2011) 51, 760 – 771. Recent Advances in Data, Text, and Media Mining; Information Issues in Supply Chain and in Service System Design.

[55] Liu, D.R., Lin, C.W., Chen, H.F., "Discovering role-based virtual knowledge flows for organizational knowledge support," *Decision Support Systems*, (2013) 55, 12 – 30.

[56] Senator, T.E., "Link mining applications: Progress and challenges," (2005) SIGKDD Explor. Newsl. 7, 76–83.

[57] Harper, W.R., Harris, D.H., "The application of link analysis to police intelligence," *Human Factors* (1975) 17, 157–164; Chen, H., Chung, W., Xu, J.J., Wang, G., Qin, Y., Chau, M., "Crime data mining: a general framework and some examples," *Computer* (2004) 37, 50– 56.

[58] Sparrow, M.K., "The application of network analysis to criminal intelligence: An assessment of the prospects," *Social Networks,* (1991) 13, 251 – 274

[59] Boongoen, T., Shen, Q., Price, C., "Disclosing false identity through hybrid link analysis," *Artificial Intelligence and Law* (2010) 18, 77–102

[60] Reid, E., 2003. "Using web link analysis to detect and analyze hidden web communities." *Information and communications technology for competitive intelligence,* (2003) 57–84.

[61] Zhou, Y., Reid, E., Qin, J., Chen, H., Lai, G., "US domestic extremist groups on the web: link and content analysis," *Intelligent Systems*, (2005) IEEE 20, 44–51.

[62] Grau, L.W., "Something Old, Something New. Guerillas, Terrorists, and Intelligence Analysis. Technical Report," *Army Combined Arms Center* (2004)

[63] Grau, L.W., "Something Old, Something New. Guerillas, Terrorists, and Intelligence Analysis. Technical Report," *Army Combined Arms Center* (2004); Popp, R., Armour, T., Senator, T., Numrych, K., "Countering terrorism with information technology," *Communications of the ACM* (2004) 47, 36–43.; McCulloh, I.A., Carley, K.M., Webb, M., "Social network monitoring of Al-Qaeda," *Network Science* (2007) 1, 25–30.

[64] Boongoen, T., Shen, Q., Price, C., "Disclosing false identity through hybrid link analysis," *Artificial Intelligence and Law* (2010) 18, 77–102.

other applications in competitive[65] intelligence.[66] An important product of link analysis combined with other methods is information rich 3D graphics.[67]

Intelligence using social media has been a growth area.[68] All of these studies, and others not mentioned, have made great progress in using social media to find out about the users, and many times about their behavior. But as we shall see next, asyngnotic networks operate in a different way, and so unless significantly extended or improved, the techniques developed so far are not sufficient to handle the full needs of intelligence analysis. Without new techniques of analysis, asyngnotic networks will remain invisible.

Using Neuroscience Models to Understand Asyngnotic Networks

Asyngnotic networks have several characteristics that are somewhat different from other networks. As the structure and behavior of asyngnotic networks constantly are in flux, it is difficult to predict how they work or when they will strike. They are self-organizing, so any action may not be driven by a detectable dispatch of a leader's command. Instead, they act as if triggered by an unknown force. As notions of leadership theory applied to any

[65] Vaughan, L., You, J., "Content assisted web co-link analysis for competitive intelligence," *Scientometrics* (2008) 77, 433–444.; Ramakrishnan, T., Jones, M.C., Sidorova, A., "Factors influencing business intelligence (BI) data collection strategies: An empirical investigation," *Decision Support Systems* (2012) 52, 486 – 496.

[66] The study used web co-link analysis to generate competitive maps in the WiMAX industry. Reid (2003) identifies seven techniques of competitor analysis including *a*) advertising analysis; *b*) alliance networks analysis; *c*) competitor profiling; *d*) corporate culture analysis; *e*) futures-based analysis; *f*) media analysis; and *g*) opportunity assessment.

[67] Risch, J.S., May, R.A., Dowson, S.T., Thomas, J.J., "A virtual environment for multimedia intelligence data analysis," *Computer Graphics and Applications, IEEE* (1996) 16, 33–41; Chin, G., Kuchar, O.P., Whitney, P.D., Powers, M.E., Johnson, K.E., "Graph-based comparisons of scenarios in intelligence analysis, in: Systems, Man and Cybernetics," 2004 IEEE International Conference on, IEEE. pp. 3175–3180.; Chung, H., Yang, S., Massjouni, N., Andrews, C., Kanna, R., North, C., 2010. VizCept: Supporting synchronous collaboration for constructing visualizations in intelligence analysis., in: IEEE VAST, pp. 107–114

[68] There is an important discussion regarding privacy in the United States and how to balance it against national security. *See* Omand, David, Jamie Bartlett, and Carl Miller. "A balance between security and privacy online must be struck." Magdalen House 136 (2012); Jaeger, Paul T., Charles R. McClure, John Carlo Bertot, and John T. Snead. "The USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and information policy research in libraries: Issues, impacts, and questions for libraries and researchers." *The Library* 74, no. 2 (2004); and Rovner, Joshua. "Intelligence in the Twitter Age." *International Journal of Intelligence and CounterIntelligence* 26, no. 2 (2013): 260-271

organization hold that leadership is essential to its growth and effectiveness, the fact that asyngnotic networks operate without leaders raises the question: "If there is no leadership, then how does the asyngnotic network operate and organize itself?" Since there also is no consistency in communication pathways informing these networks, they may operate in a way that is invisible to traditional link analysis that depends on pre-identified nodes to "link" with common characteristics usually found through multi-linear regression. Since their membership is not known, traditional social media data mining tools are not as helpful. There is no "consciousness" in the network as it is formed, and network formation is not driven by any strategy. Another part of the mystery involves the constant change and propagation of asyngnotic networks. What causes these changes, how do the changes take place, and what are the forces that provide the energy for propagation?

Hebbian Plasticity

As asyngnotic networks operate in a way that is not unlike the phenomenon associated with neurons found in the brain, we may look to neuroscience as a reference framework for analysis. By transplanting into the intelligence world models that describe the behavior of neurons, we can better locate and understand the behavior of asyngnotic networks.

The Hebbian plasticity model[69] refers to how the brain learns by strengthening links between different neurons by constantly "re-wiring" itself. This phenomena occurs naturally without leadership or direction. At the core of this model is the effect of "action potentials"[70] flowing from one neuron to another. The more flow, the stronger the link. Analogously and with reference to Hebbian plasticity, an asyngnotic network's ability constantly to change shape and configuration as it remains embedded in society is facilitated by the constant flow of action potentials from one network node to another. In neuroscience, these "nodes" are neurons; in an asyngnotic network, they are individuals or component organizations that in counter-terrorism parlance typically are referred to as "cells". In the world of neuroscience, the action potential is measured in millivolts, but in the intelligence world, we will need to define these flows with reference to flows of communications (emails, messages, telephone calls) or memes.[71] The flow of

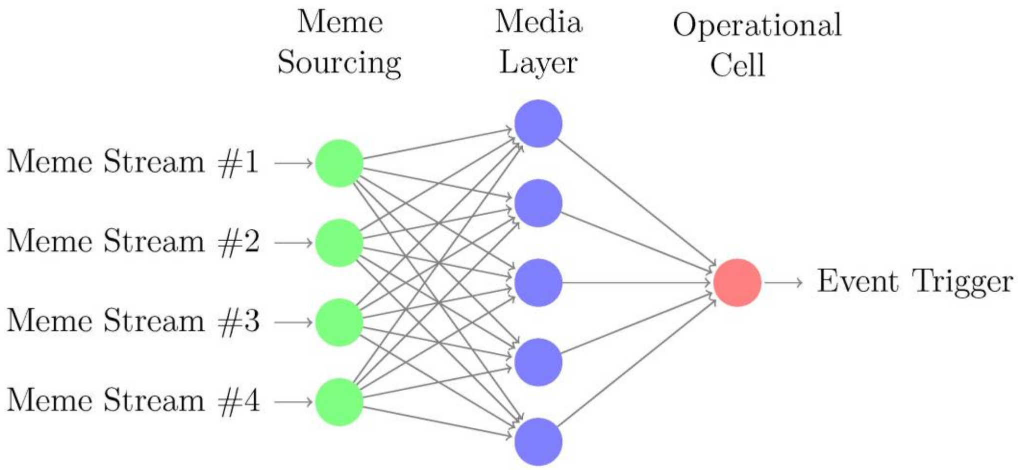
[69] Hebb, D.O., *The Organization of Behavior*, Wiley (1949)

[70] An action potential is the change in electrical potential associated with the passage of an impulse along the membrane of a muscle cell or nerve cell.

[71] Memes are an element of a culture or system of behavior that may be considered to be passed from one individual to another by nongenetic means, especially imitation. Its

memes is able to traverse the restrictive boundaries of any fixed communication system. For example, memes can flow through the open mass media as a type of signaling (*see* Figure 1).

Figure 1: Meme Flows through Media.



In an asyngnotic network, streams of memes flow through the system at unpredictable rates, and are aggregated in each operational cell. If the level of meme stimulation equals or exceeds a threshold $\Diamond$, then the cell will trigger an event, which would be an attack or any act in furtherance of a conspiracy.

The Hebbian plasticity model compels one to examine asyngnotic networks by assessing the strength between different nodes in the network. Since more meme flow means more strength connecting the nodes, and since any node can be connected to any other node, it is crucial to find the strongest connections. These stronger connections may highlight enough of the shadow of the asyngnotic network to make it possible to detect.

Another application of the plasticity concept is in understanding how asyngnotic networks learn and remember. This is made possible through the stimulation and resultant strengthening of links between nodes caused by an above average flow of memes. In the Hebbian concept, the "cell assembly" is caused by repeated internal communications. In the intelligence world, "cell assembly" would refer to the organizational structure of the terrorist or criminal asyngnotic network.[72] Memory, which we can equate to the

origin is μιμεμα (that which is imitated).

[72] *See* also Kohenen, T., "Self-organization and Associative memory," 1989 Springer-

development of a sense of mission and shared goals by network members, is made possible by the repeated stimulation of these connections so that they have a type of reverberating activity. As a consequence, if any of the networked nodes are stimulated by a matching meme, then the entire network can become activated.[73] The fact that stimulation of one highly-linked node will trigger action potentials in other highly-linked nodes is the model of network memory. The stimulation of a node that is enough to trigger action or memory happens when the level of meme flow crosses a crucial threshold. This causes an action potential, which in intelligence terms would refer to a part of the asyngnotic network taking specific actions in furtherance of a conspiracy or carrying out a terrorist act.[74]

The Linear-Threshold Model for Network Decision Making

Another approach can be used to approximate decision-making in these networks. Using the McCulloch-Potts approach[75] it is possible to model a simple computation (decision to act) made by a network node. This is done by summing up all inflowing memes and expecting the node to take action if a threshold were reached. One complication of this approach from the SIGINT point of view is that it does not distinguish between different meme flow rates and the fact that nodes receive memes from multiple paths (sources; communication channels; media).

To think of this asyngnotic network as a decision making organization, one only needs to think of the flowing memes as being “0” or “1” which corresponds to false and true or “do not attack” and “attack”. The linear-threshold model is useful for taking into consideration the relative strength of different pathways that transmit memes to an asyngnotic node. Since nodes in a terrorist network receive messages either by traditional tradecraft routes or through general impressions from the mass media, this model allows analysis to set a value to multiple types of channels.

If intelligence is continuously monitoring a flow of memes over multiple paths, then the stimulus can be graded along a continual scale, rather than

Verlag, Berlin.

[73] This has a strange parallelism to the work by on viral phenomenon in social media in which the opinions of one person become good predictors of others in the same network. *See* Chesney, T., 2014. Networked individuals predict a community wide outcome from their local information. *Decision Support Systems* 57, 11 – 21.

[74] See the appendix for more on the mathematical expression of this model.

[75] McCulloch, W.S., “The brain computing machine,” *Electrical Engineering* (1949) 68, 492–497.

using only "true" or "false". This would allow, for example, the frequency and emotional content of messages to be accounted for. In addition, since the monitoring would be continuous, then the effect on the cell receiving the memes can be tracked over time, and thus at each instant. One nice aspect of this approach is that using historical SIGINT data combined with records of actions, it should be possible to quantify the θ value for a terrorist cell or any other node in an asyngnotic network. The McCulloch-Pitts approach likely would help explain instances of "self-indoctrination" in unexpected places, such as the recent scandal at the École d l'Air in France where in April of 2015, it was discovered that several students of the French Air Force Academy were planning to place bombs in a local mosque. Interviews revealed that their motivations were entirely self-generated.

Perceptrons and Neocognitrons

The perceptron model[76] and its progeny were developed as an explanation of visual perception. The model involves multiple layers of neurons, with the first layer being the input and the last the output. In neuroscience, the output is equivalent to recognition of an object. Here we will equate recognition to an event trigger for an asyngnotic network node that causes an overt act in furtherance of a conspiracy, an enabling action (propaganda, logistics support) or a criminal act including terrorism itself. Incoming memes flow through a number of network layers, but no meme in itself is enough to pull the trigger. At each layer in the network, the memes are processed in parallel, but as they move through multiple channels.

Because no meme in itself is sufficient to trigger an overt act, no emerging act can be anticipated if SIGINT processing does not employ this multi-channel cascading model. One SIGINT advantage to the perceptron model, however, is that it is necessary to model and process meme flows in only one direction. Each node has orientation selectivity,[77] and will pass on a trigger signal if the level of memes is sufficient and the total exceeds the threshold. A crude analogy to this is a keyword listening program. These nodes can also be thought of as filters; everything but a meme stream carrying the correct

[76] Rosenblatt, F., "The perceptron: a probabilistic model for information storage and organization in the brain," *Psychological Review* (1958) 65, 386; Rosenblatt, F., "Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms," *Technical Report Report* (1961) No. VG-1196-G-8. Cornell Aeronautical Laboratory, Inc.. Buffalo, NY.

[77] Hubel, D.H., Wiesel, T.N., "Receptive fields, binocular interaction and functional architecture in the cat's visual cortex," *Journal of Physiology* (1962)160, 106–154.

DOI: http://dx.doi.org/10.5038/1944-0472.8.3.1448

orientation will be filtered out. There is another analogy to this in decision-making theory in which it is assumed that actors systematically will ignore information that disagrees or is inconsistent with their preconceived notion.[78]

As a consequence, in the perceptron model, the final trigger is fired when there is a recognition caused by compatible, and logically inter-locking meme streams. The level of memes passing through to the next layer with a high threshold node can either be non-selective or simulate a logical AND operation requiring the receipt simultaneously of multiple (but different) memes. If the node has a low threshold, it operates as a logical OR function, because any one of a variety of memes can reach the threshold. Therefore, by modeling nodes in a perceptron sequence, it is possible to have AND layers followed by OR layers or any combination thereof.[79]

In order to use this model for intelligence, it is necessary to identify the meme components graded by intensity of each trigger and classified according to logical interconnectivity. Learning these recognition patterns can happen only by use of historical meme flow data tied to a specific trigger and overt act. The underlying framework of the neocognitron model[80] should be useful as a starting point for meme-trigger analysis.[81]

Aggregate Characteristics of Asyngnotic Networks

Several characteristics distinguish an asyngnotic network from other more structured networks, making this phenomenon extremely difficult to monitor and control. Perhaps the most important distinction is that asyngnotic networks are self-organizing knowledge networks which enable a "meme" or stimulus (i.e., event, idea, or image) to pass through a group or community in

[78] Cook, M.B., Smallman, H.S., "Human factors of the confirmation bias in intelligence analysis: Decision support from graphical evidence landscapes," *Human Factors: The Journal of the Human Factors and Ergonomics Society* (2008) 50, 745–754; Nickerson, R.S., "Confirmation bias: A ubiquitous phenomenon in many guises," *Review of General Psychology* (1998) 2, 175.

[79] Note that when nodes are linked together in an asyngnotic network, it is possible to produce any function of Boolean logic e.g., AND, OR, NOT, or XOR. See appendix for more on the mathematical expression of this model.

[80] Fukushina, K.M., "Neocognitron: a self-organizing neural network model for a mechanism of pattern recognition unaffected by shift in position," *Biological Cybernetics* (1980) 36, 193–202

[81] See also the LeNet approach by LeCun. (LeCun, Y., Boser, B., Denker, J.S., Henderson, D., Howard, R.E., Hubbard, W., Jackel, L.D., "Backpropagation applied to hand-written zip code recognition," *Neural Computing* (1989) 1, 541–551). There are a number of other neuroscience models that can be considered such as pattern completion, interference between different "cell assemblies" and synaptic loops.

an unstructured way. As the name implies, these networks provide a vehicle for the expression of emerging—often unconscious—ideas, feelings and motivations among network members. Since asyngnotic networks are not permanent, they form and dissolve as the stimulus proceeds leaving few traces beyond an affective residue in those touched by the process. Thus, in some ways the spread of a meme through an asyngnotic network is like the spread of a virus through a population; and like a virus, the meme changes as it emerges and has different effects on those it encounters.[82]

This evolutionary property of asyngnotic networks is one reason why they are so difficult to identify and map. The social media analysis and linking techniques discussed above focus on the flow of information (or memes) within and between individuals and groups, which assumes a more defined target (meme) and more structured relationships than are typically found in an evolving asyngnotic network. This does not, however, mean that these techniques are without merit. Since asyngnotic networks support the emergence of sometimes unconscious and latent feelings toward a particular idea, image or subject, they are not in themselves vehicles for action. Instead, any triggering action results from the transmission of the meme through other, more established subsystems, which may be more amenable to being surfaced using current intelligence tools. The residue of the asyngnotic network may become visible when one or more members of an existing (online or other) community are triggered by an emerging asyngnotic meme so as to actively plan and communicate within the group their pending reactions. Thus, in terms of the neurological models discussed above, an asyngnotic network may alter (i.e., lower or raise) the action potential within an established community by impacting the willingness of members to engage (or dis-engage) in action of some kind.

Until recently, asyngnotic networks would have been considered informal social networks for sharing ideas and "news" within a closed community. As such, the techniques discussed above would provide a valuable window into the fairly well defined or semi-permanent relationships between cells or individuals. The emergence of these networks, however, is a consequence of ongoing advances in telecommunications and social media that allow members of any given community to be concurrent members of any number of unrelated groups. As a result, a meme can travel through the global population (consciousness) in a discontinuous, unpredictable way, jumping

[82] This is not unsimilar to the "telephone" game in which persons pass from one to another a sentence, but as it is passed along, it is changed.

from one network to another, leaving multifarious effects within the specific communities it touches. In other words, the same meme may have vastly different impacts on the individuals and communities it reaches. For example, it might cause the temporary linkages of networks, even when prior to that time there was no planned or realized connection. This partially explains how self-organization works.

The flow of memes can be powerful. For example, the ISIS beheading videos leave an indeterminate affective impression on the individuals who view them. They educate and influence, but without any advance planning of a target for their influence. These videos stimulate a wide range of possible reactions from the various established networks exposed to them. These might range from the subsequent actions of Anonymous to the increased solidarity of Islamic groups, to a call for peace from religious groups or skepticism from the diplomatic community.

In short, asyngnotic networks represent a significant advancement in human communication by allowing the real-time transmission of ideas and images (memes) simultaneously among billions of persons. These networks are largely resistant to language and other traditional barriers, and are only likely to become more important as more people are linked together through the mobile Internet and social media. Given the present global institutional structure and political economy, the emergence of a global (mass) consciousness largely resistant to overt or covert leadership might pose the greatest threat to established interests and the laws that protect them as well as pose a challenge to national security.

Practical Application of the Asyngnotic Network Approach: Charlie Hebdo

In Paris, on January 7, 2015, Cherif and Said Kouachi, two Islamic terrorists murdered the staff of the satirical magazine *Charlie Hebdo* using Kalashnikov assault rifles. In leaving the criminals shouted "We have avenged the Prophet Muhammad." In their escape, the criminals stopped their vehicle to get out and shoot a police officer who was lying wounded on the ground. Approximately 3 km away, they abandoned their car, which later was found to be stuffed with Molotov cocktails and jihadist flags. At the same time in south-west Paris, Amedy Coulibaly shot a 32-year-old jogger in the Fontenay-les- Roses park. About two hours later, the Hebdo terrorists used their

Kalashnikovs and rocket-propelled grenade launchers to rob an Avia petrol station near Villers-Coutterest, north-east of Paris.[83] The next day in the morning another criminal weilding a machine gun and pistol shot dead Clarissa Jean-Philippe, a young policewoman in Montrouge. By this time, the police had identified the two Hebdo murderers and issued an arrest warrant. One of the terrorists had been jailed in 2008 and had been known for a long time for militant activities. They took refuge in the Creation Tendance Decouverte print shop in Dammartin-en-Goele.

At 5:00pm, the Hebdo terrorists ran out of the building, guns blazing, and were shot dead. At the same time, after another shootout, two other terrorists Amedy Coulibaly and Hayat Boumeddiene took hostages at a kosher supermarket in Porte de Vincennes (in the east of Paris). They demanded freedom for the Hebdo terrorists (thus showing a connection between the two events), but were killed approximately 15 minutes after the Kouachi brothers, miles away. The police were given a chance to attack when the terrorists paused to pray. They left in their wake four dead. Hayat Boumeddiene escaped to join the genocidal ISIS group in Syria, but *later* was linked to the original Hebdo terrorists by more than 500 telephone calls. Supposedly the Hebdo attack was in response to an incitement to murder issued by a religious authority somewhere, but that does not explain killing the young policewoman or going after a Jewish supermarket. Omer el-Hamdoon, president of the Muslim Association of Britain defended the murders and claimed that publishing cartoons was not covered by freedom of speech, and this was echoed in the Egyptian press and elsewhere.[84]

Only two weeks later, terrorists opened indiscriminate fire on a café in central Copenhagen to kill the Swedish cartoonist Lars Vilks. The two criminals escaped in a Volkswagen. Shortly thereafter, a security guard working at a synagogue was murdered, and two police officers wounded by another gunman. This attack followed the same pattern as in Paris: First, murder cartoonists; then murder Jews. One gunman was shot dead by police the next morning.[85] In Paris, 17 citizens and three terrorists were dead; in Copenhagen 2 citizens and one terrorist were dead. In Copenhagen, the

[83] Location 49 03'46.92" North; 2 41'38'60" East.

[84] Penketh, A., Weaver, M.,."Charlie Hebdo: first cover since terror attack depicts prophet Muhammad," *The Guardian* (2015), Online version.

[85] For a timeline of the cartoon-related violence incidents, see: Staff, R., "Timeline - Prophet Mohammad cartoons bring attacks to Scandinavia," *Reuters* (2012) Online version.

Danish intelligence agency (PET) reported that one of the terrorists (the one still at large) had been on their "watch list".

It is difficult to know what intelligence could have done in advance to stop the Hebdo attack. Immediately speculation started regarding the affiliation of the terrorists. Were they part of the so-called Islamic State (ISIS), or part of al-Qaida (AQ), or part of a subsidiary of AQ, or perhaps members of AQ in the Arabian Peninsula (AQAP)? Much of the analysis seemed to be after the fact. This is the opposite of intelligence, which by definition must complete its analysis *prior* to any event. Judging by the statements made afterwards, it is clear that the extent of analysis was confined to compilation of watch lists of people who were not watched and little more.

In order to employ an asyngnotic network approach to develop intelligence on terrorist groups, it is necessary to link the abstract and ephemeral nature of these networks with the physical reality of terrorist operations on the ground. The asyngnotic network approach would start by recognizing that all terrorist cells are each but one *node* in a complex living system that is interconnected with other networks, mostly invisible. For example, it is clear that since the terrorists were able to obtain heavy artillery, they were in contact with networks that provided financing, other networks that provided training, and yet other networks that provided logistics and distribution of terrorist equipment. This is the physical layer of the terrorist organization.

One way to link asyngnotic networks with this physical reality is to utilize Living Systems Theory (LST), developed by James Grier Miller, a former OSS officer who went on to play a major role in social science. In Table 1 (above), we have listed the twenty categories of subsystems defined by LST and then matched them against the types of intelligence technologies and practices that might be used to detect and monitor their associated asyngnotic networks.[86] In this way, the LST model may serve as a useful starting point to hypothesize asyngnotic networks and uncover the hidden connections that were stimulated by the flow of those memes responsible for triggering the attacks. In the next section we will discuss a few of the practical intelligence challenges in identification of asyngnotic networks.

[86] There is a fuller description of LST in the appendix.

Table 1: The Charlie Hebdo Attack. Application of the living systems model to asyngnotic network analysis. An asyngnotic network as applied to terrorism is categorized according to different aspects of a living system.[87]

Subsystem	Al Qaida Instance	SIGINT	HUMINT
Input Transducer (IP)	Lookouts, e-mail, radio, television	l,c,d,i	v
Ingestor (IN)	Banks, mule trains, recruiting camps	$,o	f,v
Internal Transducer (IT)	Monitors incoming information and interprets	i	X
Channel and Net (CN)	Phone and email receivers	l,n,v	v
Decoder (DE)	Internet, radio frequencies, messenger	l,n,$	c
Timer	Planning cells		f
Associator (AS)	Filing systems, target analysts, accountants	l,d,k,g	
Memory (ME)	File cabinets, disk drives, and keepers		c
Decider (DC)	Planners, now distributed over net	l,n	g,d,k
Encoder (EN)	Computer, video camera, radio/phone	l,c,y,i	c
Reproducer (RE)	Recruiters and disbursers	$	f,v
Boundary (BO)	Guards, sentries, walls	i,o	a
Distributor (DI)	Communicators, logistics, transport	o	s
Converter (CO)	Trainers		s,f
Producer (PR)	Bomb-makers		s,f
Storage (MS)	Weapons caches, inventories	v	v
Motor (MO)	Jets to mules	i,o	X
Supporter (SU)	Partisans & donors in host countries, news media	k,d,l,v,g	s,f,v
Output Transducer (OT)	Operatives, execution cells; three men in Paris	k,y,l,p	s,f,p
Extruder (EX)	Graveyards, jails; under internal security	o	m

HUMINT: Surveillance (s); Infiltration (f); SIGINT collection support (c); Passive monitoring (m); SIGINT: Link analysis (l); Content analysis (n); Financial flows ($); Mass media (d); Social networks (k); Cyber espionage (y); Biometrics (b); Categorization & clustering (a); Database and Big Data (g); Event detection & notification (v); Geospatial (o); Predictive modeling (p); Video processing (i). List partially derived from Popp, R., Armour, T., Senator, T., Numrych, K., 2004. Countering terrorism with information technology. *Communications of the ACM* 47, 36–43.

[87] Based on McCreary, J., 2015. For the night of 7 January 2015. NightWatch Online.

Discussion: Using the Asyngnotic Approach in Intelligence

The starting point of dealing with asyngnosis as leading to potential bad outcomes is to recognize it exists and that it enhances linear police and counterintelligence work.

The largest challenge in strategic and other kinds of warning is to "warn left of the threat." That is to say, to warn that information conditions are promoting the emergence of a threat, *before* the threat has developed. It is low probability warning because at this early stage the threat is one of many potential outcomes of visible developments. It also is the time when the emerging threat is easiest to manage.

The practical advantages of tracking asyngnotic networks are several. The historic precedents prove the value of using memes in very early identification of emerging threatening behavior before overt action has been detected. As mentioned above, the most elusive challenge in warning of violent threats has been to find a way to warn with some confidence when they are ideas before significant action begins. The purpose is to gain time and save costs in managing the threat environment. Once a malefactor starts to take action other than communications, the clock starts ticking and the costs of prevention start to rise.

A good example of asyngnotic network emergence was the unexpected appearance of flash mobs in Cairo and Alexandria that preceded the ouster of President Mubarak.[88] The flash mobs demonstrated a propensity for leaderless self-organization, at least in the initial stages. Leaders do emerge or surface quickly, but not when the mob is gathering. Somebody starts the phone-chain, but lots of other gang or cell leaders make the mob happen. They also illustrate in real life that asyngnotic networks are real and have impact, often significant.

U.S. intelligence missed the overthrow of Mubarak, in part, because it failed to recognize the importance of the flash mobs. Nevertheless, the flash mob were not the biggest impact of the memes that were floating around. The Egyptian military leadership recognized in the memes and in the mobs that

[88] Jurgenson, N., "When atoms meet bits: Social media, the mobile web and augmented revolution," *Future Internet* (2012) 4, 83–91.

they had an opportunity to push aside Mubarak because he wanted to install his son as his successor!

Warning at the stage of emergence, based on chatter and ideas, has always depended on the experienced judgment of analysts. That has seldom been a persuasive basis for action by decision makers. Before asyngnosis, there was no systematic technique for capturing that professional judgment so it could be more persuasive in justifying and targeting early prophylactic measures. Asyngnosis also provides a scaffold that enables the wisdom of experienced officers to be preserved and taught to new analysts. For example, when the probability of a cyber or terrorist threat is low, asyngnotic analysis can enable tracking the buildup or lack of buildup of mental intensity that will drive action. This helps improve the accuracy and, more importantly, the confidence of warning. As such, asyngnotic analysis is the only technique for warning based on emergence, *vs* overt action.

Intelligence Antecedents to Analysis of Asyngnotic Networks

This type of analysis rests on the shoulders of earlier intelligence work. For example, there are some aspects of content analysis as applied to propaganda that offer an antecedent to the techniques needed to analyze asyngnotic networks. Alexander George[89] wrote the seminal book *Propaganda Analysis* which described the organization and techniques use by a specialized group of U.S. propaganda analysts during World War II. This was the predecessor of the Foreign Broadcast Information Service (FBIS) and the Open Source Center.[90] That group had remarkable success estimating Nazi offensives and weapons development. They studied propaganda structures and organization, word counts, themes, the authority of the propaganda vehicle, and the frequency of repetition of the themes. They were able to establish thresholds for distinguishing deception and misinformation from real developments.[91]

[89] George, A.L., 1959. *Propaganda Analysis*. Row, Peterson, Evanston, Illinois.

[90] The work was initially set up inside the FBI.

[91] George, A.L., "Propaganda analysis: A study of inferences made from Nazi propaganda in World War II," Copyright - Copyright UMI - Dissertations Publishing 1959; Last updated - 2014-01-21; First page - n/a.; George, A.L., 1954. The Scientific Status of Propaganda Analysis," *Technical Report* P-616. "The Rand Corporation. Santa Monica"; George, A.L., 1955. "Prediction of political Action by Means of Propaganda Analysis," *Technical Report* P-779. The Rand Corporation. Santa Monica.; George, A.L., "Prediction of political action by means of propaganda analysis," *The Public Opinion Quarterly* 20, (1956) pp. 334–345.

In using George's techniques to study North Korean propaganda, intelligence analysts were able to identify the emergence of a crisis based on key word counts, repetition, frequency, placement in the propaganda, and the authority of the propaganda vehicle. For example, analysts learned that the threshold for a crisis was the appearance of a meme six times in different propaganda channels in a 24 hour period.[92] This work was done manually without the benefit of a structured analytical method, computerized assistance, or a framework such as asyngnosis.

Cyber Exploitation of Intelligence

Uncovering an asyngnotic network may be as important as identification of a leader operating in a traditional network, but may be more difficult.[93] Doing this poses a number of challenges for intelligence, particularly on the SIGINT and analytical side.[94] Judgment is important and when it becomes compiled knowledge it is persuasive. Nevertheless, the promise of computerized techniques is that they will enable the identification of thresholds for action by non-state and state actors that are not solely based on the analyst's gut feeling from reading propaganda. Finally, the use of a structured technique has special value in distinguishing genuine threats from deception, bluff, misdirection and misinformation. Computerization will allow exploitation of the benefits of Big Data in support of crime prevention and early warning.[95]

The asyngnosis approach will require the development of new language concepts and more R&D on how to analyze memes in open sources. It also will drive new ways of thinking about the linkage between memes and threatening action. Those are healthy developments because the existing techniques are not working. On the SIGINT side, there is a need for continual "flow through" monitoring or order to capture and model asyngnotic networks in real time. But in order to set up real-time flow-through, much must be discovered and calibrated so that analysis is sensitive enough to bring this phenomenon to light.

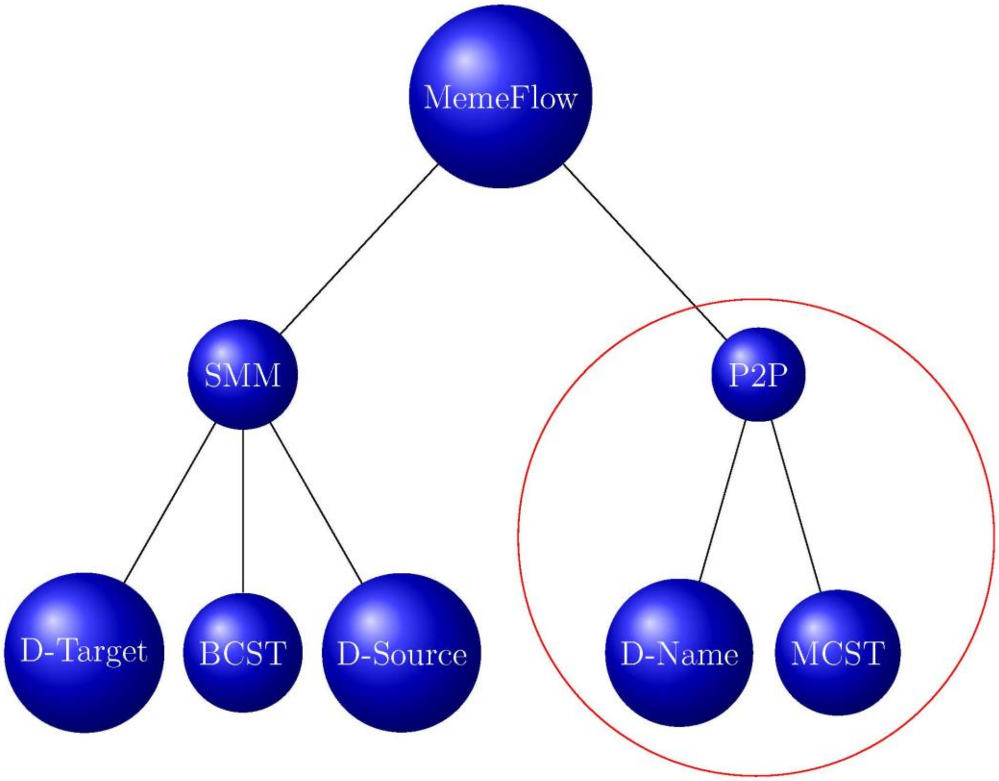
[92] George, A.L., "The Chinese Communist Army in Action: The Korean War and its aftermath," Columbia University Press, 1967, New York.

[93] The classic example of the dismantling of a terrorist network using identification of its leadership is shown vividly in the Gillo Pontecorvo directed film *La Battaglia di Algeri*, 1966.

[94] This discussion does not incorporate evaluation of the legal environment and any potential privacy issues.

[95] Big data is a general term for databases that are so large traditional processing applications are inadequate to handle them. It usually refers to the use of predictive analytics to aid in decision-making.

Figure 2: SIGINT monitoring of Asyngnotic networks examines memes flowing through both social and mass media (SMM) and Point to Point (P2).



In each of these areas in Figure 2, the meme flow can be an undirected broadcast (BCST) or multi-cast (MCST) or it can be associated with a specific target (D-Target) or originate from a specific source (D-Source) or flow to a specific person (D-Name). Traditional SIGINT monitoring is inside the red circle. Using a meme framework allows integration of social media analysis with traditional SIGINT.

Since asyngnotic networks may present rapid stand-up and dissolution capabilities, it will be necessary to develop capability to identify a network configuration as soon as it appears. After a number of these are identified, it should be possible to generate a taxonomy of asyngnotic network types. As latent asyngnotic networks may become visible then slide back into obscurity, multiple iterations of network instances might be summed to isolate latent network persistence. Frequency might initially be assumed to be synonymous

DOI: http://dx.doi.org/10.5038/1944-0472.8.3.1448

with intensity and is an important variable because in some models it may drive the node to the trigger threshold.[96]

The definition of memes may be problematical, but any result must include a classification schema. Minimal factors for classification might be:
a) incitement to specific acts; *b*) examples and "teaching" of specific acts, (but without direct incitement); *c*) logical arguments and Weltanschauung triggers; specific anti- or counter-regime assumption criticism and reframing; *d*) argument assist techniques such as "but what about".[97] Allowing networks such as ISIS to post repulsive videos on websites or through social media may aid in collection of that intelligence needed to identify and disable hidden networks. A crucial factor in success will be choosing the best asyngnotic network to analyze initially. Operationalization and calibration of multichannel indexes to substitute for the flow of "actions potentials" will be crucial. There are at least three variable classes to consider: *a*) channel characteristics; *b*) meme classes; and *c*) meme frequency and intensity.[98]

Conclusion

In this paper, we have discussed the problems of asyngnotic networks and identified a shortcoming in literature and practice regarding their analysis. We then suggested that a neuroscience approach will be useful as an explanatory framework because it assumes that the same type of self-organization and triggering functions can be models for asyngnotic networks. Finally, we discussed some of the challenges for intelligence, particularly for SIGINT, in using these models. There are many more models that can be

[96] It might be assumed that in the general media, this is easily defined by the common news cycle from output, to peak propagation, to decline and there are many off-the-shelf tools that already make these calculations. Nevertheless, it will be necessary to cluster related stories in order to estimate aggregate meme propagation trajectories. In the P2P directed channels, traditional SIGINT measures should suffice.

[97] "But what about" is a popular social media propaganda and trolling technique. *Example:* "Russia is complicating solution of the Syrian problem because of its continued support for the Assad government." Refrain: "But what about US support for the non-democratic Saudi monarchy?" The point is to drive attention away from the original idea.

[98] Johnson (Johnson, R., "Developing a taxonomy of intelligence analysis variables," *Studies in Intelligence* (2003) 47) presents a taxonomy of variables used in intelligence analysis including *a*) systemic variables; *b*) systematic; *c*) idiosyncratic; and *d*) communicative, asyngnotic networks require careful attention to a different set of variable parameters. Because of the multi-channel nature of an asyngnotic network, the testing and variable calibration must be able to encompass several types of meme flows including *a*) close circuit broadcasts; *b*) point to point directed and names; *c*) social and mass media general; and *d*) social and mass media general directed targeted. *See* Figure 2. NB: the class of media general directed source is excluded because it is too obvious.

harnessed to surface asyngnotic networks, but we hope this short discussion has stimulated discussion regarding the potential for this approach.

Appendix A. Full Statement of Anonymous[99]

Greetings citizens of the world. We are Anonymous. Operation ISIS Continues. First, we need to clarify few a things. We are: Muslims, Christians, Jews. We Are hackers, crackers, hacktivists, phishers, agents, spies, or just the guy from next door. We are students, administrators, workers, clerks, unemployed, rich, poor. We are young, or old, gay or straight. We wear smart clothes or rugs. We are hedonists, ascetics, joy riders or activists. We come from all races, countries, religions, and ethnicity. United as one, divided by zero. We are Anonymous.

Remember: The terrorists that are calling themselves Islamic State, (ISIS), are not Muslims! ISIS. We will hunt you, take down your sites, accounts, emails, and expose you. From now on, no safe place for you online. You will be treated like a virus, and we are the cure. We own the Internet.

We are Anonymous. We are legion. We do not forgive. We do not forget. Expect us.

[99] This is a transcript of the full statement from Anonymous released with its reports on #OpISIS.

Appendix B. Symbolic Notation

The notation for Hebbian Plasticity and McCulloch-Pitts can be adapted for quantitative analysis of social media and other content.[100]

Note: The notation for standardized link analysis has been excluded since it is widely published and known.

Hebbian Plasticity for Asyngnotic Terrorist Networks

This refers to the assumption that the brain or asyngnotic organization learns through the repetitive stimulation and resulting strengthening of linkages between nodes. It is given by $\Delta W_{ij} \propto xi \;\; x_j$ where *i* is the previous network node and *j* is the downstream node. As a result, W_{ij} becomes proportional to the statistical correlation between the activities of *i* and *j*. Co-variance is another way to state Hebbian Plasticity. The covariance rule is $\Delta W_{ij} \propto (x_i - < x_j >)(x_j - < x_i >)$ with $< x_i >$ being the average activity for node *i*. In this approach, *Wij* becomes proportional to the covariance between the activities of nodes *i* and *j*.

Adaption of McCulloch-Pitts

McCulloch-Pitts uses θ as a surge parameter with inflowing memes being either stimulating or general and thus being coded in a binary manner as "0" or "1". The node takes action when the threshold is met. By connecting one node to another, intermediated by meme flows, it is possible to estimate whether any node will take action. The linear threshold (LT) model uses $x_i(t+1) = H\left(\sum_{j=1}^{N} W_{ij} x_j(t) - \theta_j\right)$ which allows for a variety of incoming memes at a specific time $x_1(t), x_2(t) \cdots x_N(t)$ with each meme being valued at "0" or "1" representing regular information or other information that is stimulating to the node to take action (such as launch an attack at time $(t + 1)$). Each arriving meme is multiplied by the Hebbian strength of the pathway it arrives on. As long as the sum is less than the threshold, then there is no action taken. But if the value either reaches or exceeds the threshold θ, then

[100] *See* for example Stanley Wasserman & Katherine Faust, Social Network Analysis: Methods and Applications, Cambridge University Press, 1994, pps. 71-83 for (1) graph theoretic notation (single relation; multiple relations); (2) sociometric notation; and (3) algebraic notation. For applications, *see* Xu, J.J. & Chen, H., CrimeNet Explorer: A Framework for Criminal Network Knowledge Discovery, *ACM Transactions on Information Systems*, 23(2), April 2005, pp. 201-226; Link Analysis Workbench, Air Force Research Laboratory Information Directorate, Rome Research Site, Rome, New York, September 2004.

DOI: http://dx.doi.org/10.5038/1944-0472.8.3.1448

it will trigger the node to take action. The continuous model of the same is given by $\tau \frac{dr(i)}{dt} + r_i = F\ (\sum_{j=1}^{N} W_{ij}\, r_j - \theta_j)$ where τ is a constant and rj is a graded variable rather than a binary variable, so it responds to the frequency of communication or intensity of the incoming memes.

Nodes

Nodes can be thought of as parts of a networked organization. Generally, they are either individuals or organizations themselves as the unit of analysis.

Memes

A term that refers to communication of ideas. In a model of asyngnotic networks that has a neuroscience orientation, the flow of memes is equated with the flow of the action potential along the pathways linking one neuron to another.

Appendix C. Uncovering Asyngnotic networks using Living Systems Theory (LST)

Further evidence that complex human networks may undergo a type of self-organization is found in a branch of science called general systems theory.[101] Much of this work focused on identifying universal principles of systems that are equally true whether applied to living organisms at the cellular level or at the level of human society. In the Living Systems Theory (LST) model, networks operate as self-organization systems.[102] The LST approach came out of general systems research that developed an extensive vocabulary to discuss organizations.[103] In the LST model, there are nineteen critical subsystems divided into three classes: *a*) systems that process both matter-energy and information; *b*) systems that process matter-energy; and *c*) systems that process information. By dispensing with the matter-energy subsystems, we are left with nine subsystems that pertain only to processing of information including: *a*) Input Transducer (IP); *b*) Internal Transducer (IT); *c*) Channel and Net (CN); *d*) Decoder (DE); *e*) Associator (AS); *f*) Memory (ME); *g*) Decider (DC); *h*) Encoder (EN); and *i*) Output Transducer (OT).[104] Adding the timer completes the list of twenty subsystems.

[101] The concept of a system involves control, if there is no control, then there is no system (Hammond, D., Wilby, J., "The life and work of James Grier Miller," *Systems Research and Behavioral Science* (2006) 23, 429–435).

[102] James Grier Miller was the creator of LST. He served in the OSS. *See* Miller, J.G., "My role in the assessment program of the Office of Strategic Services," *Behavioral Science* (1996) 41, 245–261

[103] Robbins, S.S., Oliva, T.A., "The empirical identification of fifty-one core general systems theory vocabulary components," *Behavioral Science* (1982) 27, 377–386.

[104] *See also* Miller, J.G. Mater-energy processing subsystems. The extruder. *Behavioral Science* 38, 46-57 for the extruder matter-energy processing system, which may be thought of as waste by-products; the producer (Miller, *Ibid,* The Producer, pp. 46-57) who synthesizes materials internally for the network; the ingestor which would include recruitment and gathering of resources for the terrorist network (Miller, *Ibid*, pp. 10-18); the distributor which would include logistics (Miller, *Ibid*, pp. 19-32); the converter storage; motor; and the supporters which would include sympathetic persons in the community. All of these appear in the 38th volume of *Behavioral Science* (1993).

DOI: http://dx.doi.org/10.5038/1944-0472.8.3.1448