The Emergence of Global Grey Eminence (GGE) and the Future of Intelligence

Alejandro López-Chicheri

Henley-Putnam University

Professor Gary F. Bowser, Committee Chair

Dr. Harry Nimon, Subject Matter Expert

Professor Praveen Abhayaratne, Committee Member

November 23, 2014

Thesis submitted in partial fulfillment
of requirements for
Master of Science in Intelligence Management
Abstract

The objective of this thesis is to use predictive analysis to explore the potential emergence of hidden or less obvious intelligent organizations, people or machines that may be in a position of power due to their ability to gain intelligence from key organizations, people or machines that hold or produce knowledge.

The analysis identifies the technical prerequisites and global trends that may be influencing the emergence of those intelligent organizations, people or machines described from now on as Global Grey Eminence (GGE). An adequate anthropological model of human behavior involving competition and cooperation is used to scrutinise potential candidates that may emerge as GGEs in the complex global network of digital knowledge. The results also infer how the craft of intelligence may evolve in the near future to serve a GGE.
Dedication and acknowledgement

To Liza and Nicolas for their patience; to Committee Chair Professor Gary F. Bowser and Dr. Harry Nimon for guidance and expertise; to Professor Praveen Abhayaratne for sharp observations; and to all of those who kept secrets worth keeping.
Table of contents

Abstract ................................................................................................................................. ii
Dedication and acknowledgement ....................................................................................... iii
Table of contents ................................................................................................................ iv
List of graphs ....................................................................................................................... vii
Terms and acronyms ............................................................................................................ viii

Chapter 1 Introduction to the research question ............................................................... 1
Who is really in charge? ...................................................................................................... 1
  Is knowledge overpowering violence and wealth? ........................................................... 1
  The tacit nature of the intelligence of the crowd ........................................................... 4
Who may be in charge in the near future? .......................................................................... 5
  Harnessing the intelligence of the crowd ....................................................................... 5
  The emergence of a Global Grey Eminence (GGE) ........................................................ 6
  The accountability problem in a complex world ............................................................. 7

Chapter 2 Literature Review .............................................................................................. 8
Mapping the intelligence of the crowd .............................................................................. 8
  The data explosion ........................................................................................................... 8
Complex systems unpredictability: The need for enhanced data and computing .......... 12
  Technical prerequisite 1: Enhanced data or the Semantic Web .................................... 12
  Technical prerequisite 2: Enhanced computing or the intelligent machine .................. 13
Trends influencing the GGE hypothesis ............................................................................ 16
  Trend 1: Manning, Assange and Snowden: Black swans of GGE ................................. 16
  Trend 2: Open source (OSINT) vs. proprietary intelligence: The Freedom of Information
  Movement ....................................................................................................................... 18
  Trend 3: Covert vs. overt collection: To give or to be taken from? ............................... 19
  Trend 4: Anonymity vs. Authority: The Internet as the “tank in your bedroom” ............ 19
  Trend 5: Geo-localized vs. ubiquitous intelligence ....................................................... 21

Chapter 3 Research questions, methodology and limitations ......................................... 23
Research questions .................................................................................................................. 23
Methodology ........................................................................................................................... 23
Limitations of the research ...................................................................................................... 24

Chapter 4 Discussion .............................................................................................................. 25
The search for an evolutionary model ....................................................................................... 25
Competition and cooperation within human groups: Why are groups important? .......... 25
  Assumption 1: Competition trumps cooperation ................................................................. 26
  Assumption 2: Cooperation driven by benefit ................................................................. 26
Quality and quantity of the ideal data potentially useful to GGE ....................................... 27
  Data quality will remain a challenge ......................................................................................... 27
Enhanced computing may spur the emergence of a sentient GGE ............................................ 28
Will a sentient computer make the human brain obsolete? ..................................................... 30
Progress and projections in hardware: .................................................................................. 30
Progress and projections in software ..................................................................................... 34
Built-in behavioral constraints for sentient machines ............................................................. 36
Quantity of the data collected will increase despite global resistance .................................. 37
  Signs of potential corporate GGE focus on wealth ............................................................ 37
  Signs of potential GGE focus on violence ......................................................................... 38
Clandestine competition vs. overt cooperation or clandestine cooperation vs. overt competition? .................................................................................................................. 38

Chapter 5 Conclusions ............................................................................................................ 41
Three GGE scenarios ............................................................................................................. 41
  Scenario I: The omnipresent inspector at the Panopticon .................................................. 41
  Scenario II: The omniscience of the Pythia at the Oracle of Delphi ................................... 42
  Scenario III: The rogue runaway Deus ex machina ......................................................... 43
The future of the intelligence professional ............................................................................ 44
  The Quantnalist (QuA) ......................................................................................................... 45
  The NewLuddites (NewL) .................................................................................................. 45
  The dirt digger or the golden retriever (DrtD or GldnR) ..................................................... 46
  The Online Camouflage Officer (OCO) ........................................................................... 46
  The Misinformation Officer or Troll (MOTroll) ............................................................... 46
  The Global Surveillance Engineer (GSE) .......................................................................... 46
  The Global Data Sourcing Manager (GDSM) .................................................................. 47
The Treasure Hunter (TH) ........................................................................................................47
The Grassroots Terabyte (GT) ..............................................................................................47
The Senior National Intelligence Technical Consensus Holder (SNITCH) ......................48
The GGE revealed..................................................................................................................48

References..................................................................................................................................50
List of graphs


Graph 5: Historical evolution and projections of Retail PC hard disk capacity (in GB) using Moore’s Law assumptions (Computer Memory (GB) capacity duplicates every 2 years at equal cost) ......................................................... 31

Graph 6: Projections on how long an advanced computer system could simulate brain activity in real time using Moore’s Law assumptions (Computer Speed duplicates every two years at equal cost) ......................................................... 33

Graph 7: Projections on how long an advanced computer system could reach the human brain’s number of synapses using Moore’s Law assumptions. (Computer capacity duplicates every two years at equal cost) ......................................................... 34
Terms and acronyms

**Camarilla:** Spanish diminutive for cámara (lobby), a set of people surreptitiously influencing state affairs or decisions of any higher authority (RAE, 2013).

**Clandestine HUMINT:** Any HUMINT activity or operation sponsored or conducted by an organization, person or machine with the intent to assure secrecy or concealment (ODNI, 2008).

**Complex Systems:** Systems consisting of diverse and autonomous but interrelated and interdependent components or parts linked through dense interconnections which cannot be described by a single rule and whose characteristics are not reducible to one level of description. They exhibit properties that emerge from the interaction of their parts and which cannot be predicted from the properties of the parts (WebFinance Inc., 2011).

**Data:** Facts and statistics collected together for reference or analysis (OUP, 2014).

**Emergence:** The process of coming into view or becoming exposed after being concealed (OUP, 2014).

**Global Grey Eminences (GGE):** Those not-so-obvious intelligent organizations, people or machines that might be in a position of power due to their ability to gain intelligence from key organizations, people or machines that hold or produce knowledge.

**Guerrilla:** Spanish "little war" (RAE, 2013), the chosen form of decentralized combat at which Spaniards excelled for millennia, characterized by but not limited to a lack of an apparent or palpable organization and structure, extraordinary mobility and resilience, unpredictability, pervasiveness, and creativity.

**Human Intelligence:** A category of intelligence derived from information collected and provided by human sources (ODNI, 2006).

**HUMINT²:** Human Intelligence (HUMINT) emanating from the billions of human interactions online.
**Information:** Facts provided or learned about something or someone; data as processed, stored, or transmitted by a computer (OUP, 2014).

**Intelligence:** The ability to acquire, understand, and apply knowledge and skills (OUP, 2014).

**Internet Intelligence (INTINT or INT²):** An acronym I have coined to describe all sources of intelligence obtained from digitalized knowledge available on the Internet, including digital Open Source Intelligence (OSINT), Signal Intelligence (SIGINT), Image Intelligence (IMINT), Human Intelligence (HUMINT), and all other intelligence sources, provided that they are digitalized and accessible online by overt or clandestine methods.

**Internet:** A global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide; a network of networks that consists of millions of private, public, academic, business, and government networks—from local to global scope—that are linked by a broad array of electronic and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support electronic mail (ITU, 2013).

**Knowledge:** A piece of information, a thought or a belief that tracks the truth (Nozick, 1981).

**Meme:** (noun) a unit of cultural transmission or a unit of imitation (Dawkins, 1976).

**Overt:** Activities that are openly acknowledged or attributable to an organization, person or machine, including those designed to acquire information through legal and open means without concealment. Information may be collected by observation, elicitation, or from knowledgeable human sources (ODNI, 2008).

**Power:** A complex strategic situation in a given society (Foucault, 1976).

Chapter 1
Introduction to the research question

Who is really in charge?

Is knowledge overpowering violence and wealth?

Humanity now stands 14 years past the dawn of a new millennium at a challenging crossroads. At seven billion, the Earth’s population will continue to grow over the next century and likely reach the 8.3 billion mark in 2050 (UNDESA 2013, p. 4). As a consequence, it is expected that demands for food, water and energy will grow by approximately 35, 40, and 50 percent respectively (NIC, 2012), dramatically increasing pressure on the planet.

Despite current technology, humans are unable or unwilling to use Earth’s resources in a sustainable manner, opening up the possibility of the emergence of a dystopic state where the basic needs to sustain human life on the planet for the entire population are at risk (Meadows, Randers, 2012). There is a realistic and serious risk of increased poverty, inequality and exclusion, potentially leading to a rise in greed-fueled conflicts among nation states. This is especially possible given the myopic tendencies of national actors to resolve global challenges based on archaic 19\textsuperscript{th} century sociopolitical models based on a monopoly of violence.

This outdated model of resolving conflict has been the practice since the surge of modern nation states. These nation states have tended to gain control over a given territory and population through various means such as the suppression of the expression of individual violence in the citizenry through, for example, prohibiting duels and eroding the right to bear arms. Another means of gaining control is through the development of
mechanisms to regulate or coerce human relations within a territory through extensive civil and penal codes and the investment in the mechanisms of enforcement such as police forces and standing armies (Weber, 1919).

Even when national actors attempt to interact peacefully on the international scene, they are often still responding within the confines of the above-mentioned model, plaguing international organizations and political systems with coercive power struggles, political exclusion and veto (Rudzinski, 1951). In many cases, nonviolent consensus processes are underfunded, rendering the knowledge and consensus derived from them underutilized, unleveraged, or unrecognized. Under the antiquated nation state model with its implicit leadership, limited emergences do indeed emanate, but they are characterized by a lack of tangible leadership.

 Nonetheless, at the dawn of the new millennium, we can observe that some global actors are producing identifiable emergences. A recent study titled “The Network of Global Corporate Control” (Vitali, Glattfelder & Battiston, 2011) shows how transnational corporations are forming a giant economic “super-entity” with a small tightly knit core of financial institutions efficiently cartelizing a large part of global wealth.

Thanks to the telecommunications revolution as well as the development of the Internet, a global civil society is starting to emerge. According to the 2013 report of the World Economic Forum (WEF), through these communication tools, “the power of the individual as a virtual citizen is on the rise… and the speed of information transfer has shifted the paradigm of citizen expression…[creating] non-hierarchical communication structures…[as] one result” (WEF, p. 15). Billions of people digitally interacting on a
global scale through the Internet can be perceived as resulting in the emergence of a type of global conscience. Both state and wealth actors are gathering information on those interactions in order to gain tactical or strategic superiority and awareness. However, the clout is shifting back to those billions of interacting human brains. For instance, authors such as Alvin Toffler (Toffler, Longul, & Forbes, 1981) propose that we are witnessing a third wave of influence based not on violence or wealth but primarily on knowledge (See Graph 1).


Admittedly, global violence remains a pressing issue. After the end of World War II, we have witnessed a myriad of localized conflicts, many involving proxy or asymmetric warfare and/or terrorist tactics. Major world geopolitical players such as the United States and China, and to a lesser extent Russia and the European Union, are now increasingly and directly engaging in a new type of war in which the plunder is knowledge (Anthony, 2014). Either to secure strategic political intelligence, steal intellectual property, or gain competitive advantage over other nations or economic
groups, Cyber threats are becoming ubiquitous and both the United States Department of Defense (DoD) and the Federal Bureau of Investigations (FBI) have identified them as the top upcoming security threat, surpassing even the threat of terrorism. In this silent but pervasive conflict fought over the world digital networks, the influence is gained through means other than physical violence.

**The tacit nature of the intelligence of the crowd**

Simultaneously, the world’s civil society is not only capturing but also generating increasing quantities of knowledge. Similar to ants building a nest, billions of individual interactions online are creating massive pools of data and metadata that can be perceived as a global consciousness in the making. Seen from a distance, the emergence of this data lacks an apparent structure. Still, the extraordinary mobility of thoughts in the form of posts, calls, emails, tweets, and memes, together with their unpredictability, pervasiveness and creativity, mimics characteristics traditionally attributed to the spontaneous way a Guerrilla army operates, where nobody seems in charge but the parts are still able to operate and cooperate in an effective manner to achieve common objectives. For instance, during the Arab Spring, social media and the Internet were important tools for the success of the revolution, particularly in Egypt. There was not a clear leader but rather several parts coordinated by individual interactions, allowing the crowd to achieve the objective of overthrowing the regime. This is a remarkable example of the power of an emerging global consciousness.

The characteristics of the crowd’s intelligence emergence can be compared to the patterns of a highly mobile starling flock. With no apparent organization, these birds tacitly know how to move in synchronization in order to avoid hitting each other. Even
when no one bird seems to be in charge, the flock is highly effective in defeating a predating falcon. The latter, operating as a centralized weapon, does not have the slightest chance of winning (Ventoso, 2007). Just as a flock of starlings is capable of creating extraordinary collective responses, the equipped emerging crowd may be to a certain extent capable of responding as a whole against a common real or perceived threat.

**Who may be in charge in the near future?**

**Harnessing the intelligence of the crowd**

Bird watchers worldwide, confronted with these highly mobile decentralized and apparently chaotic bio patterns, have developed SIGINT solutions to track them and attempt to understand their behavior. The implications of this self-organized emerging power, which simultaneously generates data and increases knowledge, has not gone unnoticed by wealth or state actors. Former United States National Security Advisor Zbigniew Brzezinski (2010) perceives the crowd’s intelligence as “a universal awakening of mass political consciousness” mainly caused by “the nearly universal access to radio, television and increasingly the Internet that is creating a community of shared perceptions” (Brzezinski, 2005, p. 41). Furthermore, the inadequacy of the falcon confronting the starling flock is highlighted in his recognition that “major world powers, new and old, also face a novel reality: while the lethality of their military might is greater than ever, their capacity to impose control over the politically awakened masses of the world is at a historic low” (Brzezinski, 2010).
The emergence of a Global Grey Eminence (GGE)

Though Brzezinski implies that State domination is no longer possible because of accelerated social change, he also contemplates opportunities for control. In his book *Between two ages: America’s role in the technetronic era*, he notes as early as 1970, the gradual appearance of a more controlled society dominated by an elite unhindered by the restraints of traditional liberal values that “… would not hesitate to achieve its political ends by using the latest modern techniques for influencing public behavior and keeping society under close surveillance and control” (Brzezinski, 1970, p. 97).

According to Michel Foucault (1976), power is not an institution, a structure, or a certain force with which certain people are endowed; it is the name given to a complex strategic situation in a given society. Assuming that knowledge is the new power, the aim of this thesis is to speculate about or discover who currently holds these strategic positions of power in the universe of global knowledge and who may hold these positions in the future.

The historic challenge is that these influence nodes often operate behind the scenes in an unofficial or non-public capacity. This hidden phenomenon is well established and identified in many cultures. For example in the Spanish Royal Court, *camarilla* (little lobby in Spanish) was the name given to a group of advisors effectively acting as the controlling power behind the throne due to their access to the rooms, and therefore the conversations, that took place on the way to the Great Hall. In Anglo-Saxon cultures, the XVI century Medieval Latin *lobium* or covered portico on the way to the cloister is the origin of the English word lobby, a group of people seeking to influence decision makers on a particular issue given their level of access to the court. In France, that concealed position of power evolved during the XVII century into the idea of the
Éminence Grise (grey eminence in French) represented by the omnipresence of Cardinal Richelieu’s chief intelligence officer, François Leclerc du Tremblay a.k.a. Père Joseph (Huxley, 1941). Finally, in Japan, these hidden influencers were called *kuromaku* [黒幕] (Black curtain in Japanese). These examples serve to illustrate the widespread existence and even formalization of behind-the-scenes sources of power and influence based on knowledge.

**The accountability problem in a complex world**

One potential danger is that these discrete but knowledgeable influential players do not necessarily hold formal offices or have any official authority and are, therefore, not held accountable for the effects of their advice and actions. Considering the multitude of global predicaments facing humanity today, including overpopulation, inequalities and subsequent conflicts for scarce resources, identifying these emergent hidden intelligent nodes of global influence and directing them towards good advocacy may eventually lead to sound policies that serve us all.

In addition to attempting to identify the emerging players, simply exploring the patterns of emergence of hidden entities in positions of power due to their ability to gain understanding from key organizations, people or machines that hold or produce knowledge may provide fresh perspectives to official policy makers and advocates and result in significant progress in the field of strategic security.
Chapter 2
Literature Review

Mapping the intelligence of the crowd

The data explosion

Traditionally, empirical studies of influence relationships between global actors have been limited in depth because of their sole reliance on an analysis of the data of heads-of-state and governmental officials (Kegley & Wittkopf, 1976). Most recent studies have also been limited, either in scope by analyzing only the interaction of transnational companies (Vitali et al., 2011) or in size by considering only the competing interactions of a few actors (Mesquita, 2010).

However, in our day and time, by harnessing the power of open source digital data and metadata available in real time on the Internet, it is increasingly possible to find more meaningful emergent behavior stemming from the complex adaptive system of human online interactions. Every day the Internet carries between 1,453 (Cisco, 2014) to 1,826 (NSA, 2013) Petabytes ($10^{15}$ bytes) of information between computers, generating a global connected zeitgeist that has prompted a novel field of study that finds meaningful signal intelligence by using the pool of open source data, metadata, content, and statistics created by the interactions of millions of humans online.

During the last decade, the growth of the Internet has enabled the emergence of surprising new forms of collective intelligence (Malone, Laubacher & Dellarocas, 2009) and authors such as Pentland (2014) are using the term social physics to describe a quantitative science that explores how information and ideas flow and affect people’s behavior. For example, the emerging science of social physics, by collecting and
analyzing big data on human interactions, can provide insight into how ideas spread in this interconnected network and infer how groups of people make decisions across disciplines such as health, finance, and politics. Furthermore, it is now possible to mine the web in order to predict future events (Radinsky & Horvitz, 2013), and scholars are exploring how to best use semantic analysis of web data to detect emerging conflicts (Johansson & Brynienlsson, 2011).

In the field of politics, by combining research in computer science with sociology and political theory, researchers have been able to accurately measure public opinion and predict election outcomes by examining and quantifying social media communication on Facebook or Twitter (Rojas, 2013).

Furthermore, data emanating from Twitter has been successfully used evaluate, predict and detect events across a wide range of disciplines. Twitter data has been used, for example, to evaluate online public diplomacy (Fisher & Montez, 2011), predict variations in stocks (Bollen, Mao, & Zeng, 2011) and detect religious polarization in a given geographical area (Weber, Garimella, & Batayneh, 2012). Recently, a group of researchers led by S. Moat (2013) at the Warwick Business School were able to find patterns that link the evolution of the stock market with the number of visits to financial pages of Wikipedia, giving them early warning signs of the evolution of market fluctuations and providing them with a seriously competitive advantage over other players interacting in the complex market system (Moat et al., 2013).

In the field of health, using data generated from Google, other scholars have also been able to map web semantics to track the spread of airborne contagious diseases (Ginsberg, Mohebbi, Patel, Brammer, Smolinski, & Brilliant, 2009) and to obtain a
reliable and valid measurement of issue salience in the area of agenda-setting theory (Scharkow & Vogelgesang, 2009).

Analyses have also been made of actual public agenda aggregate data by looking at queries to the Google search engine (Scharkow & Vogelgesang, 2011), in addition to accurately forecasting private consumption (Schmidt & Vosen, 2009) and calculating the current level of economic activity in a given industry in real time (Varian, 2009).

These examples show that researchers are able find meaningful signal intelligence by tapping into the massive and publicly available sets of data and metadata emanating from billions of different human online interactions. That data is duplicating every two to seven days (Finley, 2011), giving rise to the concept of the Internet as a global brain which transcends the sum of its parts.

However, even when researchers have access to the explosion of open source data, much of the available data does not have shared measurements or conjoining sources. It is common to deal with data that is incomplete, non-homogenous, lacking in consistency or unable to be connected with other data due to incompatibility or lack of standards.

To combine metadata emanating from different platforms used by different constituencies with different numbers of users in different geographical areas using different languages may lead to undetectable errors both in the integrity of those datasets and the results emanating from the experimental model. Depending on the study and experiment considered, online signal intelligence success, meaningfulness and validity fluctuates from non-conclusive (Johansson & Brynielsson, 2011) to somehow accurate (Fisher & Montez, 2011; Varian, 2009), to meaningful and accurate (Bollen et al., 2011;
Ginsberg et al., 2009; Radinsky & Horvitz, 2013; Moat et al., 2013; Rojas, 2013; Weber et al., 2012).

On the other hand, it is not surprising that the most successful data experiments use normalized sets of data emanating from a single large platform such as Google (Ginsberg et al., 2009; Scharkow & Vogelgesang, 2009; Scharkow & Vogelgesang, 2011; Schmidt & Vosen, 2009), making the results more consistent and meaningful. Similarly, more consistency was found in data analyzed from Wikipedia (Moat et al., 2013) and Twitter (Bollen et al., 2011; Fisher & Montez, 2011; Rojas, 2013; Weber et al., 2012) than was found in a combination of data emanating from several online platforms (Johansson & Brynielsson, 2011).

Admittedly, predictive analysis using large set data and metadata emanating from the Internet is a new discipline, so algorithms need to be improved to be able to foresee how a social situation may evolve. Even though no one predicted emerging social movements fueled by the use of social media such as the Arab Spring, subsequent data analysis conducted a posteriori has shown paths of emergence of the event that was about to happen. For instance, a study based on millions of communications charted the deteriorating national sentiment ahead of the revolutions in Libya and Egypt (BBC, 2011). In other experiments, using a compilation of six months of publicly available data from the Global Database of Events, Language, and Tone (GDELT), investigators were able to track and map how violence moved into Afghanistan from the shared Pakistan border region (Leetaru, 2014). Using similar methods, Leetaru was also able to pick up early clues about Osama Bin Laden’s likely hiding place within a 200–kilometer radius area in Northern Pakistan that included Abbotabad (BBC, 2011).
Complex systems unpredictability: The need for enhanced data and computing

All of these research studies must deal with a part of the global network of online human interactions that is considered a complex system. Nevertheless, it is a system that can be mapped due to its high degree of connectivity, and while it may not seem organized, it most certainly is. Among other characteristics, the system displays evident neighbor interactions along with pattern recognition, feedback, and indirect control qualities (Johnson, 2001), all evidence pointing to self-organization.

Even though the system is observable and able to be mapped, its non-linear structure means that traditional tools such as algebra or other forms of logical inference may not be useful to predict what form the emergent set might take from the initial set of conditions (Long, 1994). The global network of online human interactions is difficult to model or to predict using the tools and rules of logic.

Although it is entirely possible to observe a complex adaptive system, it remains difficult to calculate emergence. For this reason, an actor willing to harness the system’s emerging knowledge may not be able to exercise the powers of prediction unless the actor can enhance the quality and quantity of the data captured and/or the actor’s own ability to process it into knowledge. For this reason, some prerequisites would increase the chances of a GGE.

Technical prerequisite 1: Enhanced data or the Semantic Web

Currently, on the visible Internet, most human interactions are dominated by unstructured and semi-structured documents. Experts such as Berners-Lee (2006) are advocating for a collaborative movement within the Internet to allow it to evolve into a web of linked data or a Semantic Web in the form of “…a common framework that
allows data to be shared and reused across application, enterprise, and community boundaries” (W3C, 2011, p. 1). The final objective is to better enable computers and people to work in cooperation allowing the machine to understand the human as opposed to the current paradigm where the human still tries to understand the machine (Berners-Lee, Hendler & Lassila, 2001). A Semantic Web would result in far superior sharing of data.

**Technical prerequisite 2: Enhanced computing or the intelligent machine**

Another prerequisite is to increase the machine’s ability to process data and knowledge faster, by enlarging its computing capacities. Following Moore’s Law, which was initially predicted by the computer scientist in 1969 and refined during a 2005 interview, the long-term trend in the history of computing hardware shows that the number of transistors that can be placed inexpensively on an integrated circuit has doubled approximately every 18 months, and most of the computer industry technology road maps confirm that the trend is still active (KTH, 2009).

However, while his prediction has proven to be accurate, Moore admits that there is a limit to it and concedes that the law may not apply indefinitely, noting that transistors will eventually reach the limits of miniaturization at atomic levels. Still, he is sure that “we’ll find ways to squeeze even further than we think we presently can” (Moore, 2005, p. 2).

Furthermore, research commissioned by the Joint Economic Committee of the United States Congress foresees that nanotechnology and human “…enhanced abilities to understand and manipulate matter at the molecular and atomic levels are promising a wave of significant new technologies over the next five decades” (Kennedy, 2007, p. 1).
These new understandings may lead the way to the possibility of a technological singularity in the form of greater-than-human intelligent machines with the ability to unexpectedly reshape our future (Eden, Moor, Søraker, Steinhart, 2013).

Ray Kurzwei, the new Director of Engineering at Google Inc., is also contemplating the potential of greater-than-human intelligence. According to his more realistic predictions, “…computers are on the threshold of reading and understanding the semantic content of a language.” He admits that the computer does not read at the same level of understanding as humans, but goes on to claim that “…since they can read a million times more material than humans, they can make up for [understanding] with quantity” (Cadwalladr, 2014 p. 1).

Yet the question remains if those enhanced machines would be ever capable of forming new thoughts, understanding human emotions, personality traits, or human decision-making, unless algorithm for these processes are factored in and tested.

While it is true that we cannot predict how a human establishes a new idea, concept or thought, it might be possible for a computer to predict trends not for individuals—as a previously non-existing idea cannot be generated—but for the statistical or semantic analysis of aggregated ideas emanating from the intelligence of a crowd acting in a synchronized manner online.

It is likely, therefore, to assume that in the near future, “…artificial intelligence [will advance] to a point where computers enhance and accelerate scientific discovery and technological change…producing discoveries that are too complex for humans” (Fisher, Selin & Wetmore, 2008, p. 7). Researchers predict, in fact, that “…there are no fundamental limits to what can be achieved,” due in part to the absence of a “…physical
law precluding particles from being organized in ways that perform even more advanced computations than the arrangements of particles in human brains (Hawking, Russell, Tegmark & Wilczek, 2014), when those processes and arrangements are finally revealed.

The reality of machines surpassing humans may arrive sooner than expected. Louis A. Del Monte, physicist and author of *The artificial intelligence revolution* worked for over thirty years as a leader in the development of microelectronics for IBM and Honeywell. Del Monte predicts that between 2040 and 2045, machines will outmatch human intelligence (Love, 2014).

It is plausible to assume that the world of competitive intelligence is aware of these trends and that intelligence agencies are actively exploring alternative hardware and software venues to achieve enhanced computing capacities. According to documents leaked by former United States intelligence contractor Edward Snowden, the effort to build one such machine is underway as a classified contract of the National Security Agency at the Laboratory for Physical Sciences in College Park, Maryland, part of a $79.7 million research program titled Penetrating Hard Targets (Rich & Gellman, 2014). The leaked documents show that as recently as September 21, 2011, the United States SIGINT agency was trying to assess the benefit of continuing research and whether a practical-scale Quantum Computer (QC) “could be developed within a reasonable timeframe” (NSA, 2011, p. 3), from which we can infer that a working QC was not accomplished at the moment of the writing of that confidential memo.

Nevertheless, it remains a possibility that the creation of an enhanced computer—one able to exponentially collect and process human online interactions in order to predict and provide the means to control human behavior—will exist in the near future.
Trends influencing the GGE hypothesis

Trend 1: Manning, Assange and Snowden: Black swans of GGE

Referring to the 2008-2009 global financial implosion, mathematician Nassim Nicholas Taleb pinpointed the inherent risk of trying to artificially stabilize a complex system by inhibiting fluctuations, which can result in exactly the opposite effect, as the constraints make the observer blind to largely unpredictable events known as “black swans.” In Taleb’s own words, “complex systems that have artificially suppressed volatility tend to become extremely fragile, while at the same time exhibiting no visible risks…[being] too calm and [exhibiting] minimal variability as silent risks accumulate beneath the surface” (Taleb & Blyth, 2011, p. 1).

This may precisely have been the case for the United States intelligence community since 2001. The emerging culture of sharing knowledge inside the United States intelligence community following the lessons of September 11 led to de-compartmentalization of intelligence data, making the system more volatile and permitting Private Manning, an intelligence analyst of the lowest military rank, to gain access to all the historical Department of State confidential cables. External unauthorized disclosure allegedly supported by Freedom of Information activist Julian Assange was only a matter of time. Evidently, the inherited rigid counter-intelligence regulations and procedures, which may have historically dissuaded individuals from disclosing classified material, were not adapted or softened to match the new post-September 11 spirit. This made the risk of breaching the confidential cables virtually invisible to counter-intelligence controllers. The massive mid-2010 disclosure of United States SIGINT capacities following the persistent leaks of former intelligence contractor Snowden has
further increased the awareness of the limits of state and private actors to conduct covert electronica surveillance (See Graph 2).


Beyond the legal or moral debate, the world is starting to realize that information technologies are multi-purpose in nature. The dominant narrative emerging in the global media is that communication technologies not only can be used as covert surveillance systems by governments in connivance with commercial vendors, telecommunications carriers and Internet Service Providers, but they are being used in this manner as we speak (Google News, 2014).

One result is a decline in interest in traditional espionage represented paradoxically by the Central Intelligence Agency (CIA). In contrast, since June 2013, the previously almost unknown National Security Agency has come into the spotlight, allegedly responsible for the unlawful global mass electronic surveillance of both American and non-American citizens alike (See Graph 3).

Trend 2: Open source (OSINT) vs. proprietary intelligence: The Freedom of Information Movement

History shows that any exerted force—in this case real or perceived pervasive mass surveillance—is expected to be met with a certain level of resistance. Resistance, from the Latin re-sistere (to re-stand, to re-set) accurately describes the dichotomous relationship between the Freedom of Information Movement and governments and corporations... One version of the narrative is that powerful governments and corporations are collecting, holding, and in some cases censoring the data of humanity. Another version describes the Freedom of Information Movement as the young and defiant opinion of the people, lacking political power but nevertheless shifting towards liberalization and homogenization of freedom of information regulations, at least across democracies (Beyer, 2011).

As one of their main goals, the Freedom of Information Movement aims to maintain an open web and to provide people with the power to discover, create and contribute to the massive and publicly available data on the Internet. A key advocate of this crowd open-sourced crusade is Tim Berners-Lee, one of the fathers of the Internet.
On the 25th anniversary of the Internet, Berners-Lee asserts that the movement not only wanted to keep the Internet “non-hierarchical, decentralized and radically open,” but is also concerned with how to build systems of “…checks and balances to hold the groups that can spy on the net accountable to the public” (Berners-Lee, 2014, p. 1).

**Trend 3: Covert vs. overt collection: To give or to be taken from?**

People willing and ready to surrender personal data or metadata voluntarily to obtain a benefit is a growing trend, but these very people may fiercely object when this same data is obtained by clandestine means or if they are not aware that the collection is taking place. Many people, for example, find it disturbing that Google has distributed over a billion mobile devices installed with the Android Operating System, making it possible for a single private sector player to track the movements of one seventh of the worlds’ population. Enabling one entity to capture that much information about people is worrisome, leading prominent members of the Freedom of Information Movement to describe a simple technology such as mobile phones as “[…] tracking devices that also make calls” (Assange, 2012).

**Trend 4: Anonymity vs. Authority: The Internet as the “tank in your bedroom”**

As a result of this real or perceived threat, there is a growing awareness of the potential for the Internet to merge into one giant grid of mass surveillance and mass control using government and corporate surveillance to facilitate totalitarianism.

According to WikiLeaks founder Julian Assange, using the Internet is like “having a tank in your bedroom” (Wright, 2012, p. 1); in other words, the extreme danger that the Internet is coming to represent cannot be ignored as we go about our online business.

Many analysts are advocating for some combination of privacy protection and
government transparency (O’Hara, 2011). Paradoxically, personal privacy is a concept of declining interest in the last decade, but it still manages to generate more interest than the concept of government transparency, which jumped in 2009 but has not significantly increased since then (See Graph 4).


What are the authorities doing about protecting personal privacy of citizens?

Supra-governmental bodies such as the European Union have launched an inquiry into the Electronic Mass Surveillance of EU Citizens, inviting former intelligence contractor Edward Snowden to participate. During his deposition, Snowden called for the adoption of “pervasive, end-to-end encryption [which] can quickly make indiscriminate surveillance impossible on a cost effective basis” (Snowden, 2014, p. 9).

Likewise, the United Nations Third Committee on Social, Humanitarian and Cultural Issues has recently approved a resolution on “the right to privacy in the digital age,” confirming that the same rights that people hold offline must be protected online, including the right to privacy. Accordingly, the resolution calls upon all states:
(a) “To respect and protect the right to privacy, including in the context of digital communication;

(b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law” (UNGA, 2013, p. 2).

**Trend 5: Geo-localized vs. ubiquitous intelligence**

The information collection and privacy debate is contributing to the rise of a new privacy industry which is filling the demand gap for online privacy and reputation protection products (Kuchler, 2014). At the same time, fears of privacy loss are having an undesired effect on United States cloud service providers. The Cloud Security Alliance survey is forecasting short-term losses from $21.5 to $35 billion over the next three years (Peterson, 2013). In fact, Google, one of the largest United States-based cloud operators, has recently made an 80 per cent cut on the price of Cloud Storage Services (Google, 2014), most likely in order to retain fleeing clients.

Lone activists are not the only ones recommending more privacy protection. Advisors to the European Union addressing members of the European Parliament at the 8th Civil Liberties Committee hearing on the surveillance of EU citizens are recommending several ideas and actions that are gaining traction. For example, a consensus has been reached on the idea that the European Union should reconsider instruments of cooperation with the United States such as the Terrorist Finance Tracking Programme (TFTP) and the Passenger Name Record (PNR) agreement. The European
Union is also considering the possibility of granting asylum—in a European Union member state—to whistleblowers. Furthermore, the EU is proposing a European secure data storage location and network that would take the form of a “privacy cloud” (European Parliament, 2013). The creation of a data storage location and network has been already endorsed by Chancellor Angela Merkel of Germany as part of a broad counter-espionage offensive designed to curb mass surveillance conducted by the United States National Security Agency and its British counterpart, the Government Communications Headquarters (GCHQ) (Paterson, 2014).

Another example of state response to threats to citizen privacy is the international conference on Internet Governance hosted by Brazilian President Dilma Rousseff in April 2014, which was co-sponsored by the Internet Corporation for Assigned Names and Numbers (ICANN) and included the participation of industrial, civil society, and members of academia. Fadi Chehadé, ICANN CEO, believes the opportunity exists to “design a collaborative ecosystem of governance of global scope” (Pardo, 2014, p. 1) reflecting the overwhelming civil society consensus that the Internet be kept neutral and not be weaponized as a covert intelligence tool for the benefit of any specific nation or interest group.
Chapter 3
Research questions, methodology and limitations

Research questions

Considering the above identified technical prerequisites, trends, and assumptions, the following research questions will be examined:

1) Can we detect signals that may infer patterns of the emergence of a dominant individual or collective Global Grey Eminence with the capacity to collect and process digital intelligence from the world’s data pools and, as a result, be potentially able to influence global policy openly or behind the scenes?

2) If these signals exist:
   a) What evolutionary model may a GGE adopt?
   b) Is it possible to identify which actors could be in a position of becoming a GGE in the future?
   c) When can we expect the GGE to emerge?

3) If the emergence of a GGE is deemed plausible:
   a) How might the emergence of a GGE change the future of the intelligence profession?

Methodology

The method used in this research project is descriptive, using both quantitative and qualitative analysis. Quantitatively, the research focuses on descriptions of the progress and projections in computing hardware and software that may lead to a sentient machine. From a qualitative angle, a historical and contemporary literature review has been conducted using a wide assortment of open information sources including not only
official government and industry releases, academic papers and scientific journals, but also the latest newspapers articles, Internet search engines queries and whistleblower leaks. The intentional use of a wide variety of publically available sources that fall outside of the traditional academic realm is to keep the research as up to date as possible. Furthermore, the research is easy to verify, encouraging participation in subsequent analysis and interpretation in the ongoing speculation about the emergence of a GGE.

**Limitations of the research**

Providing that the potential emergence of a GGE would give an immense competitive advantage to the actor that controls it—similar to the power that newly weaponized technologies gave to actors in the past—we can infer that this development will be highly classified, prompting civilian and/or military stakeholders to maintain superiority by using excessive secrecy (Schwartz, 1998). This will obviously prevent public accessibility to primary sources on the subject for an unspecified period of time.
Chapter 4
Discussion

In addition to the identified technical prerequisites and trends that may influence the emergence of a GGE, it is essential to identify a valid evolutionary model in recognition of the impact that human behavior can have on the movement towards a potential GGE emergence.

The search for an evolutionary model

The collective and global scope of the hypothetical phenomena being studied merits taking into account the latest trends in human evolutionary theory influenced by the novel field of multilevel selection theory (MST). This theory explores human cooperation and competition not only from the individual point of view but also from the perspective of human groups acting as a single organism.

Competition and cooperation within human groups: Why are groups important?

David Sloan Wilson (2007) and others believe that “a major evolutionary transition occurs when the group becomes a new higher level organism” (Wilson, Van Vugt, O’Gorman, 2007, p. 1), thereby acknowledging that groups of individuals, such as bands, armies and tribes can also be considered relevant actors in the history of evolution. Wilson considers group selection more prevalent and more important than previously thought, assuming that natural selection can be meaningfully applied at the group level (Boehm, 1999; Wilson, 1997). Emanating from the core body of multilevel selection theory, the following assumptions can be considered:
Assumption 1: Competition trumps cooperation

It is evident not only theoretically but also empirically that human groups are more equipped to compete than to cooperate with each other. The competitive global corporate environment and the ubiquitous culture of team sports are both testaments to this concept. Pervasive warfare is an extreme instance of this circumstance as observed though all of human history, leading some to argue that “large-scale hierarchically complex societies arose as a result of evolutionary pressures brought on by warfare” (Turchin & Gavrilets, 2009, p. 185).

Individuals operating within groups who are more fit to compete will be in an advantageous position to exercise their power. The winners in an armed conflict gain advantage, while the losers or the less fit will suffer a decrease in leverageable power due to surrender, capture, injury and/or death. Of course, fitness to compete is no longer limited to or based on physical prowess. If we consider one definition of fitness in today’s society, education, we can speculate that a person holding an Ivy League university credential will be more likely to succeed and rise in the global network of influence than a person with the same cognitive capacities holding a credential from an obscure community college.

Assumption 2: Cooperation driven by benefit

One effect of warfare is its likelihood of making belligerent groups more cohesive internally. Warfare can be considered “an extreme form of parochial altruism, driven by the ‘cooperate to compete’ evolutionary logic” (Turchin & Gavrilets, 2009, p.185), prompting individuals to act as a team for their own advantage. Coalition formation has, been regarded as one of the most powerful strategies in competitive interactions, and
some experts believe that the evolutionary forces emerging from coalition dynamics may have been of paramount importance for the origin of our species (Alexander, 1990; Flinn, Geary, & Ward, 2005).

Nonetheless, altruism is not free. The key insight concerning individuals and groups in multilevel selection theory is that egotistic individuals have higher rates of success than altruistic individuals within groups, but groups with higher proportions of altruistic personalities are more fit than groups with relatively more egotistic members (Wilson, 1997). Consequently, an egotistic individual operating within an altruistic and cooperative group will have a large advantage over his/her peers and over members of other predominant egoistic groups, and as a result, may advance faster and move to a higher and more internally altruistic group.

However, to make it to a new higher internally altruistic group successfully, this competitive individual will perceive that in order to keep advancing, at least initially, he or she may need to cooperate and establish a stronger network, a tactic we are familiar with if we have ever taken a new job. Intergroup competition and individual inner and/or inter group cooperation and networking play a vital role in human evolutionary emergence and therefore may also play a key role on the emergence of a GGE.

**Quality and quantity of the ideal data potentially useful to GGE**

**Data quality will remain a challenge**

It has already been established as a technical prerequisite that there must be an improvement in the quality of the data in order for a GGE to make sense of it all. This can be further illustrated by looking at big data. At the moment, big data is seen as a revolutionary advance and is rightly considered an important resource, but it is not a
silver bullet. For instance, results often turn out to be less robust than they initially seem, as big data is still plagued with quality problems. Existing redundancies in the pools of data emanating from the Internet often result in deviations, making large datasets prone to undetected errors. Furthermore, while experts concede that “big data is very good at detecting correlations, especially subtle correlations that an analysis of smaller data sets might miss” (Marcus & Davis, 2014, p. 1), the sheer abundance of correlations that are found can result in the meaningful ones being lost in the haystack. Finally, big data has been proven adequate to help analyze common problems, yet often fails to help analyze less obvious or more nuanced problems.

Obviously, the problem of quality increases as the quantity of the data increases. At the moment, enhanced data initiatives aimed towards the achievement of a Semantic Web are trying to normalize and universalize datasets as much as possible, but those timid efforts may not be enough to overcome the gigantic momentum generated by the explosion of mainly unstructured data generated by billions of human daily interactions online. The fact is that data management is mind-numbingly time-consuming. Analyzing an average user’s hard drive makes it glaringly obvious that current human data generators do not have the time, inclination or incentive to follow rigid data standards and good data housekeeping off-line or on-line.

**Enhanced computing may spur the emergence of a sentient GGE**

Our second identified prerequisite to be able to gain and process knowledge explores the not-too-unlikely possibility that in the near future, enhanced computing could lead to the appearance of an intelligent or sentient machine able to process increasing quantities of human-generated unstructured data to find meaning and
knowledge in it. The National Security Agency is not alone in the search for enhanced capacities through quantum computing.

Google is currently acquiring artificial intelligence companies in the United States and abroad; and corporate insiders, on condition of anonymity, recognize that the strategic purchases are directed to improve “semantic technology and the ability to understand what people [are] asking for online and answer in a very human way.” (Bilton, 2014, p.1). Surely it is no coincidence that the search engine giant has recently hired Ray Kurzweil as the new Director of Engineering. Kurzweil is credited with coining the term “singularity” to refer to “the moment at which a computer will exhibit intelligent behavior equivalent to, or indistinguishable from, that of a human,” which he calculates will happen by 2029 (Cadwalladr, 2014, p. 1).

Some believe that singularity has already been partially achieved. For example, Watson, IBM’s cognitive technology, was able to beat human competitors in a game of Jeopardy by using statistical inferences to simulate certain aspects of human analysis (Cook, 2011). Another IBM machine, RS/6000 SP, known as “Deep Blue,” was able to win against chess world champion Garry Kasparov under tournament conditions due to the machine’s ability to process over 200 million chess positions per second. Describing his non-human rival, Kasparov conceded he could perceive “a new kind of intelligence across the table” and saw “some signs of intelligence, of a weird kind, an inefficient, inflexible kind” (Silver, 2011, p. 1) that prompted him to think that singularity still has a way to go to reach its full expression. Both experiments used enhanced computer power to process large quantities of data (IBM, 2014), the precise path a GGE may take in our hypothetical scenario of one emerging.
Will a sentient computer make the human brain obsolete?

In order to determine whether a sentient computer could render the human brain obsolete, it is helpful to understand the basics of human cognition, however according to researcher Dr. Harry I. Nimon, the process “remains scientifically undefined and not well understood. In order for an investigator to understand cognition, [he or she] must first be able to define and track the mechanics of an idea” (Nimon, 2013, p.106).

Indeed, mapping the brain is the subject of study of the Brain Research through Advancing Innovative Neurotechnologies (BRAIN) Initiative, also referred to as the Brain Activity Map Project, a major collaborative research initiative announced by the United States administration in 2013 in coordination with private sector partners such as IBM. Its aim is to map the activity of every neuron in the human brain in an attempt to mimic the success of the Human Genome Project.

While results are yet to be seen, we can speculate about how long it will take for hardware and software to emulate the human brain capacities by analyzing the overall trends, progress and projections in computing hardware and software.

Progress and projections in hardware:

Memory progress and projections

The human brain is undoubtedly the most powerful “computer” known to man, accounting for a “memory capacity of approximately 2.5 petabytes (or 2.5 million gigabytes)” (Reber, 2010). If we transpose Moore’s Law—the semiconductor industry capacity to double the number of transistors in a single chip every 18-24 months at equal cost—onto the historical progression of computer memory or gigabytes (GB), it means
that achieving a 2.5 million gigabyte memory capacity could occur by 2025 even in commercially available computer and retail products (See Graph 5).

Graph 5: Historical evolution and projections of Retail PC hard disk capacity (in GB) using Moore's Law assumptions (Computer Memory (GB) capacity duplicates every 2 years at equal cost).


Note: X =Time in years. /Y= Capacity (GB) The plot is logarithmic, so the fitted tangent corresponds to exponential growth.

Processing speed progress and projections

The historical progression of computer memory (GB) points to the possibility of a machine achieving brain capacity, however challenges remain in other aspects, notably processing speed, space, heat, and other critical factors.

Human brain nerve impulses operate on the frequency range of kilohertz (KHz), a million times slower than that of a regular home computer operating at gigahertz (GHz) speed. In spite of this speed differential, the brain of a toddler can recognize his or her mother in less than a second in dim light conditions and uncontrolled surroundings, while
the most advanced computers fail to perform this seemingly easy task. One explanation may be that the human brain has about 100 billion neurons yet many more synapses wiring these cells together (Choi 2013). The human brain generates, through these neurons and synapses, a still largely undescribed process of interaction with a multi-echeloned and non-linear structure of brain protein chains that allows the human organ to function in a more effective manner than a computer.

To put this in perspective, in the most accurate simulation of the human brain carried out to date out by the RIKEN Advanced Institute for Computational Science (AICS) using the fourth most powerful computer in the world—the Japanese K computer with over 82,944 processors—the machine took 40 minutes to complete a simulation of one second of human brain activity (Sparkes, 2014).

If today it takes 40 minutes (2,400 seconds) for one of the most advanced machines in the world to process one second of human brain activity, and assuming that Moore’s Law, which has been accurate for 45 years, will continue to be accurate, and allowing a two-year period of time for the duplication of processor speed at equal cost, we can infer that the most advanced machines may be able to process at human brain speed no earlier than 2036 and no later than 2038. At this point, we may witness the first case of authentic singularity (See Graph 6).
Graph 6: **Projections** on how long an advanced computer system could simulate brain activity in real time using Moore’s Law assumptions (Computer Speed duplicates every two years at equal cost).

Note. *X* = Time in years. *Y* = Seconds taken to process one second of Human brain activity.

Baseline starts on 2014 when K computer, SPARC64 VIIIfx 2.0GHz, with over 82,944 processors was able to process 1 second of Brain activity in 40 minutes (2,400 seconds) and ends between 2036 and 2038 when potentially if Moore’s law continues to be observed, an improved computer system may be able to process 1 second of brain activity in less than one second.

Another less optimistic way to infer speed projection is to consider the number of neurons in the human brain as ranging between 86 billion (Sukel, 2011) and 100 billion (Choi 2013) in addition to the number of connections between those neuron synapses. Current studies estimate that a “single neuron has hundreds to thousands of synapses, and that “the estimated number of these functional contacts is much higher, in the trillions,” estimated at 0.15 quadrillion (Sukel, 2011). In August 2011, IBM BRAIN Initiative efforts were able to unveil two working prototype computer processor cores amounting to a combined number of 327,680 synapses (IBM, 2011). We can infer, again using
Moore’s Law, that in order to surpass the said \((0.15)10^{15}\) or 150 trillion
\((150,000,000,000,000)\) synapses, the IBM sentient Computer efforts will achieve
singularity around August 2069 with a Cognitive Computing Chip arrangement of over
175 trillion functional synapses (See Graph 7).

**Graph 7: Projections** on how long an advanced computer system could reach the human brain’s number of synapses using Moore’s Law assumptions. (Computer capacity duplicates every two years at equal cost).

![Graph 7: Projections](image)

*Note. X = Time in years. Y = Number of synapses. Baseline starts on 18 August 2011 when IBM introduced two working prototype designs with cores fabricated in 45 nm SOI-CMOS with a total of 327,680 synapses (IBM, 2011), and ends around August 2069 when, if Moore’s law continues to be valid, an IBM Cognitive Computing Chip may reach 175 trillion functional synapses.*

**Progress and projections in software**

While IBM is still moving to achieve its “long-term goal to build a chip system
with ten billion neurons and hundred trillion synapses, while consuming merely one
kilowatt of power and occupying less than two liters of volume” (IBM, 2014), the
research on advanced software continues. Although the progress made in hardware has been remarkable, many believe that software advances have been even more significant,
with “performance gains due to improvements in algorithms…vastly [exceeding] even the dramatic performance gains due to increased processor speed” (USPCAST, 2010).

In “Solving real-world linear programs: A decade and more of progress,” Robert Bixby (2002), previously of Rice University and ILOG and now of IBM, explains that thanks to algorithm improvement, a model that might have taken a year to solve ten years ago can now be solved in less than 30 seconds. In a paper prepared for the Office of the Under Secretary of Defense for Personnel and Readiness, Lockheed Martin quotes optimization expert Martin Grötschel of Konrad-Zuse-Zentrum für Informationstechnik Berlin:

A benchmark production planning model solved using linear programming would have taken 82 years to solve in 1988 using the computers and the linear programming algorithms of the day. Fifteen years later, in 2003, this same model could be solved in roughly 1 minute, an improvement by a factor of roughly 43 million. Of this, a factor of roughly 1,000 was due to increased processor speed, whereas a factor of roughly 43,000 was due to improvements in algorithms.

(Lockheed Martin, n.d. p. 9)

Grötschel also cites an algorithmic improvement of roughly 30,000 for mixed integer programming between 1991 and 2008 (Lockheed Martin, n.d. p. 9).

Edward Lazowska, a professor at the University of Washington, concedes that the rate of change in hardware has been an extraordinary achievement but goes on to write that “the ingenuity that computer scientists have put into algorithms have yielded performance improvements that make even the exponential gains of Moore’s Law look trivial” (Lohr, 2011).
A powerful heuristic algorithm could provide a good enough solution for addressing the problem of creating a computer equal in ability to the human brain by considerably reducing the need for hardware improvements. Throughout 2013, Defense Advance Research Project Agency (DARPA) solicited information that could lead to the development of a Cortical Processor, conceding that “understanding…how the cortex works is beyond current state of the art.” At this point, “basic algorithmic principles are being identified and merged into machine learning and neural network techniques.” Based on the neo-cortex model, these algorithms can “recognize complex spatial and temporal patterns and … adapt to changing environments…[with] the potential for providing new levels of performance and capabilities for a range of data recognition problems” (DARPA, 2013).

Responding to the question of whether machines can think, Alan Turing quipped that if people cannot tell the difference, it doesn't matter. It is enough for the machine to appear intelligent if it does so in a comprehensive way (Hauser, 2013). The question of sentient computers, of course, remains elusive. Paraphrasing an anonymous source quoted by Professor of Theoretical Physics Michio Kaku in his book the future of the mind, “if our brains were simple enough to be understood, we wouldn’t be smart enough to understand them” (Kaku, 2014, p 104).

**Built-in behavioral constraints for sentient machines**

If ever achieved, sentient computer systems may also carry the common risks associated with unconstrained systems. Beyond fantasy dystopian scenarios where machines take over and annihilate the human race, there is a real-life trend in artificial intelligence to create systems to achieve “self-protection, resource acquisition, replication
and efficiency” (Omohundro, 2014, p. 303). If the system becomes independent enough or there is an absence of constraining rules, the possibility exists for the system to act in unexpected or even potentially harmful ways. In a recent interview, Steven Hawking warned that "artificial intelligence could be a real danger in the not too distant future” (Matyszczyk, 2014).

Quantity of the data collected will increase despite global resistance

For a GGE to emerge, the system will need to be able to collect massive amounts of data from key organizations, people and/or machines that gather and/or produce knowledge. Two obvious players are telegraphing a strong signal of emergence in this interception, collection and storage capacity: corporate Internet Service Providers and government intelligence agencies.

Signs of potential corporate GGE focus on wealth

On one hand, corporate Internet Service Providers (ISPs) and search engines led by the world leader Google Inc. openly collect and process the web information, not only to improve search results but to develop the ability to profile customers by crossing search queries with ISP addresses. By analyzing metadata emanating from other services such as email (Gmail) and mobile phone platforms (Android), they better target commercial advertisement (AdWords). Google does not officially release its information collecting capacity, but as of September 2008, Google was processing 20 petabytes a day (Dean & Ghemawat, 2008) and is still largely surpassing capacities of other important player such as Microsoft (Bing), Yahoo or AOL (Goodwin, 2013).
Signs of potential GGE focus on violence

Another obvious set of massive information collectors is governmental SIGINT agencies. On August 9, 2013, the NSA released a brief statement following Snowden’s disclosure. In it, the agency recognized that its foreign intelligence mission “‘touches’ 29.21 petabytes of data a day or about 1.6 percent of the Internet [world's traffic]” (NSA 2013, p. 6). According to the same publication, the total daily Internet global traffic amounts to 1,826 petabytes (CISCO, 2012), but even if this 29.21 petabytes of data per day were processed, it represents less than 2% of the total daily Internet global traffic. Still, the NSA likely “touches” as much or more data than Google (Gallagher, 2013).

Clandestine competition vs. overt cooperation or clandestine cooperation vs. overt competition?

The data collected and the intelligence processed by the NSA now represents 75 percent of President Obama’s daily intelligence briefing, according to Mike McConnell, Director of National Intelligence under President George W. Bush, and he believes that all indications are “that this percentage is only going up” (Riley, 2013). Even if this intelligence collection is critical to the strategic advantage of the United States, the overall perception is that the agency is eroding citizen rights at home and abroad. The global assumption is that the signal intelligence agency is clandestinely competing with both foreign powers and with the citizens of the United States it pledges to serve rather than openly cooperating and using this intelligence for collective advantage...

Ironically, Google is either deliberately or incidentally collecting similar amounts of data and metadata from the Internet and from user interaction with their platforms. Still, in contrast to the NSA, the Internet giant is perceived as a benign player openly cooperating to the benefit of the masses, which continue to use their search engines and
product daily in an openly competitive search engine market. The reality, however, presents Google in a different light. There are suspicions that Google may be at best unwillingly cooperating or at worst actively collaborating on developing covert capacity with the NSA (Ackerman, 2014).

It has been established that Google has clandestinely competed against their costumers by not being transparent about how much data is collected and for what purposes. It is true that Google makes data search statistics available through Google Trends and other corporate products, but to this day, Google does not publicly acknowledge the full amount of the data it collects daily from its multiple platforms; it is also true that their raw search volume numbers are not made public. They instead provide normalized search results, claiming that “doing so allows the underlying characteristics of the data sets to be compared” (Google, 2013, p. 1). Furthermore, the company does not release statistics about their different platforms in a systematic way, making general unofficial numbers available that tend to be outdated guesstimates. As previously mentioned, with one billion Android devices in the world, the folks at Google have a vast range of information on a huge portion of humanity (Gross, 2014, p. 1).

An accurate look at Google’s user base and how much interaction is conducted on their platforms needs to come from outside unbiased sources with nothing to hide, such as independent bench markers (Comscore, 2013). Google has the largest number of users by far, reaching an estimated 1.8 trillion searches last year, averaging over 5 billion search queries every day worldwide and representing a staggering 70.8% of the global search engine market share.
The seeming lack of transparency should make people wonder how all this Google-collected data is being used, if it is being used at all. A valid doubt is whether, in its quest to compete, the company may be behaving selfishly with the data collected during interaction with the human swarm. For now, the general perception is that Google’s goals are altruistic in nature, partly due to global services perks such as free mail, free storage and free search services.

Provided that the consumer benefits of using Google platforms and products compensate for any perceived loss of privacy, the general consensus is that the company helps individuals cooperate with each other, thus benefiting all participants.
Chapter 5
Conclusions

Three GGE scenarios

If a GGE were to emerge, the way that it would interact with the rest of humanity in the future is open to discussion, but we can speculate about three potential scenarios.

Scenario I: The omnipresent inspector at the Panopticon

Similar to the Panopticon, from Latin pan (all) and opticon (to observe), the prison concept devised by Social Philosopher Jeremy Bentham in the 18th century, this version of a Global Grey Eminence will allow for a very small group of custodians to monitor the rest of the population. The population will be like inmates in a semicircular penitentiary watched from an opaque center tower by a guard which can perfectly see into every cell but cannot be seen. Bentham describes the Panopticon as “a new mode of obtaining power of mind over mind” by giving the impression of the “apparent omnipresence of the inspector … combined with the extreme facility of his real presence” (Bentham, n.d, Letter, XI).

Based on a simplified model, the Panopticon Global Grey Eminence may:

- serve only a few, and intelligence emanating from it may be proprietary;
- encourage intergroup competition and only intra-group cooperation;
- prioritize covert collection above overt or transparent gathering of data;
- discourage or prohibit anonymity;
- force the world’s data to be more geo-localized and fragmented;
- focus on competitive intelligence, power, security, conflict and violence and tend to be conservative in protecting the status quo or the right “to have”;

41
• help generate an Orwellian type of society controlled by fear similar to the Big Brother described in 1984.

Scenario II: The omniscience of the *Pythia at the Oracle of Delphi*

Similar to the *Pythia* at the Oracle of Delphi, this version of the Global Grey Eminence may collaborate with individual users by sharing auguries to those in need of insight. As a motor of change, the *Pythia Global Grey Eminence* will be perceived as benign and will freely share knowledge, tending to promote social change the same way Plutarch’s ideas were beneficial to the people and which most likely came from his exposure to the Oracle he served for many years as a priest. These ideas compiled centuries later in Moralia (Plutarch, n.d.) were indeed instrumental in conceptualizing the leap of consciousness that eventually launched the French Revolution. Considering the above, a simplified model of the *Pythia Global Grey Eminence* may:

• serve the vast majority of the world’s population, and intelligence emanating from it may be open-source;

• encourage intergroup and intra-group cooperation;

• prioritize overt collection of open sources;

• allow anonymity and encryption;

• embolden people to contribute with data that will make the Grey Eminence more intelligent;

• focus on ideas, morals, liberty and the pursuit of happiness and tend to be progressive in promoting individual betterment and change or the right “to be”;

• help generate a Huxleysian type of society similar to that described in Brave New World controlled by pleasure and the fulfillment of human desires.
**Scenario III: The rogue runaway *Deus ex machina***

Similar to the cheap poetic tactic described by Horace in line 191 of *Ars Poetica*, this version of Global Grey Eminence will adopt a “god from the machine” (*Deus ex machina*) approach, solving very complex issues with superficial, false or inelegant solutions. In contrast to a strong version of artificial intelligence described in the previous scenarios, this scenario contemplates the rise of a weak version of artificial intelligence (AI) described as an “expert system that matches or exceeds human intelligence in a narrowly defined area, but not in broader areas” (Dvorsky, 2013, p. 1).

In this case, the *Dues ex machina* Global Grey Eminence may use human interactions online to reproduce a self-serving *succedaneum* or substitute for knowledge. An emerging signal of this GGE could be virtual reality technologies, meaningless social media schemes and online games, all of which capture increasing time and resources of a new generation of humans too distracted by trivialities to act for the betterment and progress of the real world.

According to this simplified model, the *Deus ex machina* Global Grey Eminence may:

- serve itself, and intelligence emanating from it may be exclusive;
- encourage intergroup and intra-group competition such as who is “happier” on Facebook;
- prioritize intelligent processing over collection, as humans, at least initially, may voluntarily surrender time and data to the Deus ex machina Grey Eminence;
- destroy anonymity due to its extended inferring capacities;
- force the world to encrypt data;
• focus on self-preservation and perpetuation at any cost and tend to be revolutionary in protecting its own integrity;
• help generate a Wachowskian dystopia similar to one depicted in the movie *The Matrix* controlled by unreality.

If unchecked, this system could end up working outside of human understanding and control. Although an ecosystem that includes humans is initially necessary and relevant to serve the Global Grey Eminence in all three scenarios, if unchecked, the *Dues ex machina* GGE could eventually manage to work outside of human understanding and control.

**The future of the intelligence professional**

The future of the intelligence professional is obviously closely linked to the evolution of intelligence itself. Considering that the Internet continues to have a deep impact in many activities and spheres of humanity, we can assume that it will also have a radical effect on the world of intelligence. Assuming that the emergence of a Global Grey Eminence is possible in the medium to long term future, it is foreseeable that the most likely dominance of INT² will lead to the enhancement of mainly two intelligence disciplines to serve it:

1) **signal intelligence** to intercept and decrypt the flow of INT²
2) and **intelligence analysis** to make sense of it all.

Considering the global trends recently compiled by *The Futurist* (2011) describing how technology will reshape human occupations and careers, we can infer that the field of intelligence will be radically transformed if a Global Grey Eminence emerges.
Consequently, we can expect a variety of new job profiles to arise in the next 20 years that will range from data interpreters to electronic surveillance ethicists.

**The Quantnalist (QuA)**

Today’s intelligence analyst may evolve into a quantitative analyst or Quantnalist and will specialize in the application of mathematical and statistical methods to gain intelligence. The Quantnalist will not write reports but will instead be tasked with the creation of algorithms that will help the GGE understand and process raw unstructured data into actionable intelligence, collecting results emanating from the Global Grey Eminence and interpreting them. A precursor of this may be already happening when opinion editorial writers collect the most valued comments on any given news event posted online, and on the next day, put those online comments together as a well-crafted first page opinion editorial.

**The NewLuddites (NewL)**

Considering that most of the intelligence will be obtained using electronic sources, the NewLuddites will be the new counterintelligence asset of any given organization. They will be privacy insurers or experts in encryption who may resort to neutralizing or destroying advanced surveillance equipment the same way 19th century English textile artisans destroyed machinery to protest and reject the advent of the Industrial Revolution. A precursor of this may be a Secret Service agent who is ostensibly in charge of setting up a special tent full of electronic countermeasures in a diplomatic salon and who allows instead for the safe conduction of confidential conversations between high ranking government officials in hostile or controlled environments.
The dirt digger or the golden retriever (DrtD or GlDnR)

Using the immense pool of personal data online, this digital archaeologist may be a dirt digger, uncovering unsavory information on a target by tracking questionable past interactions online. In a lighter version, serving the *Pythia* Global Grey Eminence model, the individual may act as a golden retriever by helping a customer to understand the future by examining his or her own or somebody else’s past.

The Online Camouflage Officer (OCO)

Considering the immense pool of online personal data, cover will be increasingly difficult to achieve by intelligence officers due to the absence of a digital footprint. The Online Camouflage Officer (OCO) will be a digital identity planner appointed to create consistent social media personas that will not compromise an intelligence officer’s concealment. Considering their expertise, they may be also in charge of astro-turfing social media networks as well as producing false flag social media operations.

The Misinformation Officer or Troll (MOTroll)

Working in close coordination with the Online Camouflage Officer (OCO) the misinformation officer will be a double agent mixed with traces of agent of influence, agent provocateur and confusion agent, what is currently described on the Internet as a “troll.” This Online Community Disorganizer will be in charge of manipulating online discussions, providing misleading information, and fabricating political influence in an area of interest to support a particular agency’s objectives.

The Global Surveillance Engineer (GSE)

A mix of an electronic or computer engineer with the skills of a United Nations diplomat, the global surveillance engineers will be paramount to the success of a
foreseeable transition from national mass surveillance systems to global surveillance systems. The Global Surveillance Engineer will most likely adopt the form of an overt double agent with double alliances. This job most probably will be restricted to people with dual nationalities and multicultural backgrounds.

**The Global Data Sourcing Manager (GDSM)**

Similar to a military quartermaster, the Global Data Sourcing Manager will make sure that the Global Grey Eminence has all the data when and where it is needed. He or she will be a data logistics expert who will be able to identify data needs and either steal or purchase databases to be processed by the Global Grey Eminence.

**The Treasure Hunter (TH)**

Similar to the Global Data Sourcing Manager, this contractor will act as a talent aggregator for external expertise and will consequently have to maintain close contact with many independent “free agents” or hackers. He or she will often go treasure hunting to hacker conventions and be the buyer of choice for software exploits and algorithms. If needed, the Treasure Hunter will also be able to assemble on short notice the multidisciplinary talent needed for the production of more sophisticated or specific cyber weapons.

**The Grassroots Terabyter (GT)**

Case officers will eventually disappear or will be transferred to the field to merge with their intelligence assets, becoming grassroot terabytes. Their language skills and cultural adaptation will improve, and they will be able to collect human intelligence with miniature sensor technology implanted under the skin with reversible surgery. These temporary cyborgs will be able to collect terabytes of data on their daily field interactions.
through undistinguishable bone pierced and tattooed equipment and sensors. A precursor of this may be the United States Marines extended on-the-field intelligence effort in Afghanistan and Iraq.

**The Senior National Intelligence Technical Consensus Holder (SNITCH)**

A mix of secular priest, whistleblower, Ombudsperson and Inspector General, this universal ethics proclaimer will make sure that there is a technical consensus on what is acceptable or not in terms of electronic surveillance. With deep knowledge of intelligence systems as well as national and international law, the SNITCH will only report to the highest authorities in the nation and will use his or her position to influence public opinion or decision making to produce results beneficial to the country’s intelligence while quickly acting to denounce any abuse of citizen rights.

**The GGE revealed**

Based on the above discussion, analysis and speculation, the likelihood of the emergence of a GGE is not implausible. An actor using enhanced data, increased data collection capabilities and increased computing power could very likely emerge as a super entity with the ability to acquire close to total awareness within this century. It is clear that the most obvious candidate for a GGE—governmental SIGINT agencies—will continue conducting surveillance mandates even if they face setbacks due to encryption and law suits.

However, corporate Internet service providers and search engines, although less obvious candidates to emerge as a GGE, will increase their surveillance and data intelligence capacities as long as users continue to willingly surrender their data and corporate actors continue to augment their portfolios of services and acquisitions. Some
among the most dominant corporate actors, who may or may not be operating in an unofficial capacity, may eventually be able to find, in this massive pool of voluntarily surrendered data emanating from human interactions online, meaningful signal intelligence that will allow them to exercise a strong influence on global policy openly or behind the scenes. That a GGE will emerge is less in doubt than whether it will be friend or foe of the rest of humanity.
References


Brzezinski, Z. (2010). *Speech at the European forum for new ideas (EFNI)*. Retrieved from https://www.youtube.com/watch?v=bHknL5z8f6k#t=70


Dawkins, R. (1976). *The selfish gene*. Oxford University Press. Retrieved from http://books.google.com.pa/books?id=EJeHTt8hW7UC&pg=PA192&dq=a+noun+that+conveys+the+idea+of+a+unit+of+cultural+transmission,+or+a+unit+of+imitation+&hl=en&sa=X&ei=3NhPU8n0IMmS0QHF8IG4Dw&ved=0CCwQ6AEwAA#v=onepage&q=a%20noun%20that%20conveys%20the%20idea%20of%20unit%20of%20cultural%20transmission%2C%20or%20unit%20of%20imitation&f=false


United States President’s Council of Advisors on Science and Technology. (USPCAST) (2010). Designing a digital future: Federally funded research and development in networking and information technology. Report to the President and Congress


