IA1 – The Technology of the Security Future

David C. Shields

CSEC 670, Section 9041

Contents

1. Introduction

Throughout its history, the United States of America has been known for its ability to accomplish its goals. It has almost always been the de facto leader in the arenas of military capabilities, international leadership and new technologies. Unfortunately, over the past decade to fifteen years, the US has begun to lose its standing among the world's superpowers in such fields as cybersecurity (Zinni & Koltz, 2009, p. 15). If the country continues to let its standing slip in this very challenging field it stands to lose more than just public approval, it may very well cost its own national security. Fortunately, the government of the USA has begun to make great strides in bridging the gaps in the field of cybersecurity and is starting to recover the losses it has witnessed in the past decade or more. The USA has made great improvements in such measures as the use of remote management technologies, real-time forensic analysis, and by prioritizing research and design but the government needs to continually increase their focus on supporting these technologies if it hopes to succeed.

2. Unmanning the Security Team

The field of cybersecurity has quickly become one of the most important fields in the world of information technology but the amount of qualified and available workers has not been able to keep up with the demand. Furthermore, enterprises are demanding more and more security projects without having adequate funding for those needs (Caballero, 2009, pp. 235-236). As a result, businesses need their existing manpower and software to do more with fewer resources than before. To compensate for this demand and to meet the needs of the ever changing security issues in the enterprise, many companies have begun to offer highly advanced remote management agents. These agents can automate security needs and reduce the manpower required to secure the enterprise (Salah, Alcaraz-Calero, Zeadally, Al-Mulla, & Alzaabi, 2013, p. 45).

Remote management technologies are not a new by any means. During the early 2000's, products such as Altiris Remote Agent (Later acquired by Symantec) and Virtual Network Computing's MyVNC were utilized to remotely control systems by technical support professionals (Richardson, Stafford-Fraser, Wood, & Hopper, 1998, p. 35).

As enterprises grow, scale and develop offices that are geographically segregated from each other, the need for remote control increases exponentially. What began as a tool for remotely offering technical support slowly evolved into remote management of information systems for such purposes as remote patch management (as is the case with such applications as Microsoft Windows System Update Server (WSUS)) or remote server monitoring (such as the case with Microsoft Systems Center Operations Manager or SCOM). It seems only natural then, that companies would turn to remote management of security controls to allow them to respond more proactively to security threats.

To illustrate the value of using remote technologies to control security of systems and further express their value, it would be wise to consider the case of a zero-day attack on a major enterprise. If an enterprise has offices across multiple locations and it is discovered that one of their network clusters has fallen victim to a zero-day attack it is only a matter of time before the remainder of their network is likely to be targeted (Street, Nabors, & Baskin, 2010, p. 188). Expounding upon this concern, if it is discovered that the proper application of a particular software patch could greatly reduce the chance for the attack to permeate to other systems, it seems only logical that the enterprise would wish to respond expeditiously.

If the enterprise utilizes remote management technologies for their security infrastructure, it is possible that a simple update to their remote management software could be used to prevent an attack. The agent could potentially check the posture of a remote asset, apply the patches necessary and notify administrative staff upon completion (Peng, Chen, Xie, Gao, & Liang, 2013, p. 1158). In this manner, an enterprise is able to perform detailed security administration for their systems without the need to actually send an administrator to the location. The lack of necessity to send a person to a remote location will increase the response time of the security team. Additionally, eliminating the time spent by a technical person attempting to send complex instructions to a non-technical user at the remote site will reduce the potential for user error. All of these considerations culminate into a leaner, more time and cost-effective security response team for the enterprise.

It is clear that the use of remote agents can generate a considerable return on investment for the enterprise but they are not without fault. For all the functional automation offered by the use of remote agents, it does not remove the human element completely.

All agent software is still dependent upon the proper creation and deployment of baselines or configuration standards by a skilled administrator (Ismail, Hajjar, & Hajjar, 2008, p. 141). It follows, then, that remote management technologies are only as effective as those that administer them. In the same scenario mentioned above in which a zero-day attack is detected and an agent is used to perform a remote update, an incorrect configuration could cause more damage than good. To this end, any enterprise that wishes to implement remote management technologies must develop policies to ensure proper configuration baselines and effective use of this technology.

The first policy that must be addressed is to determine what items that the enterprise wishes to manage remotely. Management agents run the gamut from simple patch management all the way up to Data Loss Prevention (DLP) and even baseline configuration enforcement (Ismail, Hajjar, & Hajjar, 2008, p. 148). Among the remote management tools available in the market, it is conceivable to utilize a single suite for managing almost all aspects of a system or network. However, there is yet to be a market player that truly offers a perfect fit. As a result, many vendors have gone to offering modular management tools which allow the enterprise to select the modules that most effectively meet their needs (Hockenson, 2013). Once the enterprise agrees on the extent of management, it will then need to focus on the implementation of the tools.

A critical factor in establishing a quality remote management system is being able to detect and respond to anomalies in a given information system. For instance, a particular threat to system security is likely to exhibit at least some abnormal behavior such as a sudden drop in system processing power or notable fluctuations in stability (Prowse, 2012, pp. 380-381). But if an organization does not have a baseline which shows the system's behavior in normal operations, how then will an administrator know an issue has occurred? Consequently, a major uptick in the system resources may go undetected because the business has no measurement with which to compare. It stands to reason that a policy should be implemented that will establish performance baselines so that administrators will be made aware of anomalies and perform remote management of the problem machines.

One more issue exists within the policies of remote management agents that is deserving of some attention and that is the actual management of the remote infrastructure itself.

As mentioned earlier, remote agent utilization for task automation is only successful if it is managed well. In the case of the zero-day patch, the remote agent has the potential to quickly patch a system yet this can produce false negatives which may weaken security (Peng, Chen, Xie, Gao, & Liang, 2013). In order to respond to situations such as these, the enterprise should adopt a policy of accountability in which all remote management tasks performed are verified by a human so as to confirm their application. The requirement to monitor this may create additional work for administrative staff but it will also guarantee that the security and availability of the enterprise resources is sustained.

Remote agent technologies clearly offer considerable advantages to the enterprise including expedited response to security issues, reduction of time and manpower across larger enterprises, and increased stability of the enterprise (Ismail, Hajjar, & Hajjar, 2008, pp. 147-148). Despite these advantages, they do not guarantee security without the guidance and management of dedicated and knowledgeable staff that is familiar with the proper configuration and administration of these technologies. If the enterprise wishes to succeed in their use of remote technologies, it will be quintessential to map the usage of these technologies with internal policies. If the use of the technology is not connected to the organization that will utilize it, remote agents will not be effective.

3. Forensics While you Wait

Criminals have been around for as long as history has records and crime continues to permeate society. In the digital age, crime is just as prevalent but the methods used to commit the crimes have changed. No longer are crimes contained within national borders and prosecution only required within the criminal’s country (Casey, 2011, pp. 95-96). In the vast expanses of cyberspace, there are no traditional borders to contain crime nor is there a dedicated police force to uphold justice and legal usage. Couple this fact with the persistent and pervasive access to high-speed internet even in remote countries and crime becomes an international problem with highly complex legal challenges.

A hacktivist in a foreign country can attack the IT network of a firm in the USA using any number of tools that are readily available, often using a free network to disguise their identity (Street, Nabors, & Baskin, 2010, p. 255).

If the attacker lives in Bosnia but attacks from a computer in China which is routed through several locations including Russia and Korea, it is virtually impossible to prosecute without assistance from all countries involved. Before an organization can even attempt to go after the hacktivist, they must engage in a very lengthy digital forensics process to collect proof of the attack and its origins (Casey, 2011, p. 232).

The forensic data acquisition process, especially for a large network in an enterprise can be one the most time and resource intensive processes in the entire incident. It may involve collecting data from enormous data clusters, disrupting standard business operations of servers and a sobering amount of man hours. To exacerbate the issue, many enterprises do not have their own forensic staff or have a small staff that is already under immense case load. The enterprise may be required to hire an external company to collect and review the data over a very long period of time (Orebaugh, 2006, p. 38). Yet due to the nature of the ever-fluctuating Internet and its darker denizens, even a few hours of time lost can render most of the useful data for criminal prosecution invisible or irrelevant. If the perpetrator of the attack has even a marginal amount of advanced skills, they may very well erase all tracks of their assault before it is even detected (Street, Nabors, & Baskin, 2010, p. 258) .

It stands to reason, then, that digital forensic technology in its current state is vastly ineffective at expeditious response times. Furthermore, the lack of dedicated forensic teams within a majority of enterprises causes an additional time lapse between attack and investigation. If these issues are not enough, there is a very wide knowledge gap between traditional law enforcement that are trained in criminal proceedings and the highly technical world of digital forensics (Casey, Handling a Digital Crime Scene, 2011, p. 239). When all of these separate elements are combined, it is easy to understand the depth of the challenges that must be addressed to reduce cybercrime.

In the modern digital forensics world, there have been a number of technical advances in recent years including highly detailed forensic toolkits, the use of distributed computing for large datasets, and significant improvements to e-discovery technologies (Trcek, Abie, Skomedal, & Starc, 2010, p. 1473). But among all of the technologies available to improve digital forensics, few offer as much potential to increase response time as the implementation of remote and real-time digital forensics tools.

Previously, this document discussed the usage of remote agent technologies to increase the response time and capabilities for managing remote assets. In a similar fashion, remote agents can be configured to perform remote digital forensic evaluations without requiring the physical presence of a forensics investigator (Orebaugh, 2006, p. 39). By using remote software agents to connect to systems, collect the necessary data and analyze said data, a remote investigator can analyze large datasets across disparate locations. Additionally, these remote tools can be configured in such a way that data is preemptively analyzed and potentially unwanted or unallowable information can be detected (Orebaugh, 2006, p. 40).

Time is one of the most precious commodities in a criminal case and although remote forensics analysis may reduce the travel and collection time, the use of real-time forensics may further reduce these. In the case of remote forensics, the data can be collected remotely without requiring an intense amount of hands-on work but it still must be analyzed in successive fashion. However, if an organization decides to utilize real-time forensic software, it can essentially perform live scans of data even when it is on an active machine (Adelstein, 2006, p. 65).

When using real-time forensics technology, the analyst is able to collect data from machines that are actively processing data. This analysis may be performed using a self-contained forensic laptop, a software or hardware reader or even via a real-time control software that may be activated directly or remotely (Trcek, Abie, Skomedal, & Starc, 2010, p. 1477). The use of real-time or live-box analysis allows for temporal data such as that stored in Random Access Memory (RAM), virtual paging files, temporary system files et cetera. The data contained within these constantly changing files can provide crucial evidence related to computer crimes that might have otherwise been lost (Nelson, Phillips, & Steuart, 2010, p. 135). If a similar analysis were to be performed on the computer after it had been powered off and transported to another location (also known as dead-box analysis), recovering the volatile data may prove impossible.

Despite the obvious potential offered by real-time and remote analysis forensic tools, there are a considerable number of hurdles that these methods create. In the case of remote network acquisition tools, the largest hurdle is finding a tool that can perform this task in a way that is ethical and admissible in court (Casey, Handling a Digital Crime Scene, 2011, p. 236). The integrity of the data and proof that proper chain of custody processes was followed is critical in guaranteeing admissibility.

Due to this strict limitation, the investigator must ensure that any technology they use for data acquisition follows proper evidence control processes. The best way to accomplish this is to depend on tools that are considered forensically sound (Nelson, Phillips, & Steuart, 2010, p. 93). Before selecting a toolset to be used for remote or real-time forensics, it would behoove the investigator to research companies such as Guardian Software, Paraben, or others. These companies have a strong relationship with the forensics community and with lawmakers so their software is generally accepted as admissible with most US courts.

Another matter of import is to consider the staff that will be used to manage any forensic software tools in use by the enterprise. Due to the relatively high startup costs for creating a quality forensics lab, it is often financially implausible for smaller organizations to maintain a forensics team (Nelson, Phillips, & Steuart, 2010, pp. 73-74). Additionally, if an organization does not have a large network of assets that may require forensics analysis at any time, it seems cost prohibitive to maintain such a team. If the company has a large IT department or has a considerable number of regulatory issues to be concerned with (such as oil and gas companies or financial companies) then it would be prudent to maintain such a staff. Enterprises that do have forensics teams are likely to work directly with legal teams in order to quickly collect pertinent information about a particular investigation, further accelerating the process. If the organization it too small to rationally afford such a department, there are still a wealth of consulting firms that are able to offer forensic services.

As considered with the remote management tools discussed previously, the use of real-time or remote forensics tools will fit an organization best when there are policies in place related to them. Unlike the policies for other tools mentioned, forensic policies must be concerned more with laws and regulations than remote agent technologies. The enterprise must ask itself if it must maintain Sarbanes-Oxley (SOX) compliance, Federal Information Systems Management Act (FISMA), or any number of other regulatory guidelines and plan its policies accordingly (Barker, 2011, p. 98).

The first policy that must be established in the area of forensics is the policy or policies that will meet the regulatory needs of the company. For instance, a public company would need to follow SOX compliance regarding data management and reporting as set out by their governing board (Virtue, 2009, p. 64.2).

This may also impact the manner in which forensic tools can be used to gather data and how much data can be gathered without consent of the users. If the user information gathered by real-time forensics was related to financial matters, then SOX may have additional requirements. In the case of a healthcare company, their information is strictly governed by the Health Insurance Portability and Accountability Act (HIPAA) which may require more specific limitations as to what can be transmitted via remote forensics or via real-time tools as it may contain personally identifiable information (PII) (Brusil, 2009, p. 71.5). The enterprise must execute their due diligence to confirm that they meet all standards they have agreed to or are required to adhere to.

The second policy that must be addressed by the enterprise in order to use real-time forensics or remote forensics tools is the policy which mandates the events allowable for these technologies. For instance, will a real-time analysis tool only be used when a potential incident arises or will various ‘samples’ be performed to aid in early notifications? Furthermore, if a remote forensic tool is to be used, will the agent trigger only when a forensic analysis request is executed or will it, too, perform sampling of live data? The policy of the usage of these tools must be clearly defined and explained to users of the enterprise’s systems (Orebaugh, 2006, p. 38). If the users are not informed, the enterprise faces potential legal issues about employee monitoring.

A third policy for the organization to consider is the correlation of events within the enterprise Intrusion Detection and Prevention Systems (IDPS). Many tools allow for correlation of events within a real-time forensics toolkit and the IDPS sensor network in such a way that event tracing can be established from intrusion to criminal activity concerns (Trcek, Abie, Skomedal, & Starc, 2010, p. 1473). While it is true that the organization could detect anomalies within its systems and then trigger the real-time forensics of the node they suspect to have been penetrated, such methods may be too time insensitive to effectively correlate events. The framework interlinking IDPS data and real-time or remote forensics greatly expedites the investigation process (Peng, Chen, Xie, Gao, & Liang, 2013, p. 1161). The policy itself could be used to help set goals for response and mitigation times (i.e. – security will locate and mitigate proposed risks within 30 minutes of detection). Using the proposed times, the enterprise can estimate the financial and manpower requirements necessary to meet said guidelines before the equipment or software is purchased or implemented.

Real-time and remote forensic tools offer a considerable amount of value to the discovery and resolution of criminal investigations. Due to the sensitive nature of crime scenes, an enterprise must choose the forensic technologies they use wisely and implement them just as wisely. The enterprise should consider the cost of hiring their own in-house staff to handle a large number of cases or optionally hire a forensic contractor with specialized software to assist. Also, the varying legal requirements specific to the industry (HIPAA, FISMA, SOX, and so on) to which the enterprise belongs must be considered when selecting the policies and procedures to implement. The enterprise must consider the events which make use of real-time or remote forensics and whether or not the monitoring should be per event or continually sampled throughout the life of an information system. Lastly, the enterprise must decide if they wish to relate the events on the IDPS systems with the forensics software or if doing so could cause bandwidth or legal concerns. Even though the usage of these technologies may have more stringent legal concerns than others, the proper use of such tools can greatly increase security and greatly reduce many challenges to digital forensics.

4. It’s All About Priorities

This report has already discussed two new technologies that can be used to enhance security and stability for the USA. Nevertheless, these technologies are only a few minor elements in the future of cybersecurity. The field of information security is largely an emerging market and the extents to which its technologies can be used depend a great deal on continual research and design. Historically, the USA has been a powerful player on the world stage of emerging technologies – many of which are due to its highly specialized research institutions. Even so, the USA must place more attention to prioritizing research and development in these emerging fields if it hopes to return to its former technological glory (Kuehl, 2011, pp. 40-41).

Speaking boldly about rolling changes needed in the research and design fields may provide the wrong impression of the current situation. The importance of prioritized research and design has not been lost on the US government. President Bill Clinton began the cycle of strengthening the nation’s security and enhancing its research directives by implementing Presidential Decision Directive (PDD) 63 in 1998.

PDD63 focuses on protecting the critical infrastructure of the USA and improving the collaboration of government and private agencies (O'Neil, 2011, p. 131).

Implementation of PDD63, though not the final installment of such research measures, created the groundwork for the Department of Homeland Security and for many of the sweeping security measures implemented after the terrorist attacks of 9/11. In order to increase the security of the nation, President George W. Bush signed the Homeland Security Act of 2002 into law and gave the US a major boost in shoring up its research and development economy (O'Neil, 2011, p. 132). But the majority of the aim of HSA2002 was not so much about the creation of new technologies for the US to defend cyberspace but rather to focus on creating technologies to aid in military and surveillance programs. Nonetheless, the stage was set for a more mature response to cybersecurity concerns.

The true turning point for increasing research and development came after the President's Information Technology Committee (PITAC) created a report to President Bush in 2005 expressing a concerned view for the state of US cybersecurity (Benioff & Lazowska, 2005, p. iii). The report placed considerable attention on the importance of the Networking and Information Technology Research and Development (NITRD) Program and how it could be used as an engine to increase the security of the Internet and government cyber infrastructures. It also requested considerable federal attention and funding toward pursuits of science, technology, engineering and mathematics (STEM) which it found to be quite lacking from the US perspective.

Prioritized Research & Development (PRD) is used by the government and by public and private sector organizations to develop the tools and technologies necessary to enhance the nation's security and its technological performance on a global scale. The NITRD has placed a considerable focus on such technologies as Big Data (BD), Human Computer Interaction and Information Management (HCI&IM), High Confidence Software and Systems (HCSS), High End Computing (HEC), Software Design & Productivity (SDP) and Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW) (University of Maryland University Colelge, 2012). As a result, the government feels that supporting these technologies and the organizations that wish to foster them deserves funding priority and focus more so than other fields within the computing space.

Each of these technologies offer considerable potential to the interests of the country but also entails their own unique set of challenges.

The size and scale of data and databases in use in the digital age is astounding. Small localized databases for housing information or for specific programs have developed into juggernaut systems that store petabytes of data. Enterprises have begun to focus a great deal on highly scalable cloud infrastructures that use massive amounts of resources using scalable databases. Even modern datacenters can utilize high-end clusters of databases for such things as managing storage and virtual resources (Agrawal, Das, & El Abbadi, 2011). The rate at which a single database or cluster can grow in a large enterprise scale application makes the management of database systems very challenging. Current systems are functional and manageable to allow for the processing of BD but the speed and dependability of these systems will face challenges as they attempt to meet the ever-growing demand for data storage and mining.

Despite the challenges of BD management, there is no limit to the amount of usefulness that can be found in using scalable database systems for even the largest government research projects. It is no wonder that the government expresses interest in improving the rate at which more responsive and unified BD management systems such as Hadoop can process data. The need for the government and enterprises, online superpowers such as Amazon and even scientific institutions to be able to harness this technology justifies the priority placed on its development. Yet these systems require complex data mapping technology, high-end computing systems and a score of knowledgeable engineers to run them (Agrawal, Das, & El Abbadi, 2011). With the proper amount of support from federal and educational institutions and a workforce with interest in database management, the US can reach the forefront of big data technology.

The second item of interest to the NITRD is the enhancement of Human-Computer Interaction and Information Management (HCI&IM). HCI&IM has been a consideration for many years, ever since humans began to depend on information systems to gather information, finding the best way for the human to execute tasks both simple and complex has been a major focus of study. It is thanks to the works of pioneers such as Steve Wozniak and Steve Jobs (of Apple fame) as well as the financial support of Bill Gates from Microsoft that have led the developers of information systems to create Graphical User Interfaces (GUIs).

In modern computing, developers may spend considerable amounts of time debating over the best way to create a logical way for a user to interact with their programs before they even begin creating the code that will execute those programs (Ullmer & Ishii, 2000, pp. 917-918). With each new technology paradigm that is created, the way humans interact with the technology will also change.

For a realistic example of interface changes that have drastically changed computing in the past decade, one simply needs to look at their nearby smart phone or tablet. Prior to the early 2000's, touch capable interfaces were relatively uncommon in the business world and usually were limited to only a few interfaces (such as touch-based Point of Sale systems). But upon the release of the first generation of Apple smartphones and handheld tablet devices, society became keenly aware of the importance of tactile manipulation of equipment. This precedence was so strong that it caused Microsoft. to steer away from their traditional mouse and keyboard interface and consider touchable UI (Spates, 2011).

The truly modern interfaces on software and hardware in the modern age can be controlled in many different ways. Certain technologies for use in digital phones and tablets have focused on the use of predictive text input enabling rapid input of information by contextually completing words. Other technologies have focused on using voice recognition software such as Dragon Naturally Speaking or the popular Siri digital assistant on Apple products. Office products now will offer countless templates or project options for a user to select when they begin a new processing session or easily reopen the previous project. In essence, computer software is being created with interfaces designed to greatly enhance the productivity and interaction between itself and the user. NITRD hopes to position the USA at the forefront of creating more powerful and potent ways for the user to interact with software and systems they encounter by making 'smarter' software.

One of the most stressful work environments for many humans to be involved in is the field of emergency management. When human life is at risk and unnatural circumstances are at play, it is easy for humans to struggle with clear and coherent interaction with each other and those hoping to aid. In crisis situations, people may be required to work in intense and long shifts and somehow smoothly transition control of situations to another team at the end of their shift (Carver & Turoff, 2007, p. 34).

Emergency management professionals must make truly life and death decisions often with less than satisfactory information. As a result, there is a considerable amount of interest in this field to create more automated, decision-based systems capable of analyzing hundreds of scenarios in an emergency situation. By providing certain pieces of information to a system and providing a series of parameters to meet, the human can use the computer interface to expedite quality decision making based off of given information. It is quite easy for the imagination to consider how many ways the government and defense industries could use similar technologies to aid in matters of national security.

Computer systems are capable of analyzing and reviewing massive amounts of data in a fraction of the time it might take for a human to do the same. However, the capability of such machines to make decisions and consider human factors is a cause for concern. Simply put, how can a computer system truly make decisions that require a human mind and human judgment? It is to this end that NITRD wishes to enhance the capabilities of High Confidence Software and Systems (HCSS). A computer cannot be trusted to analyze information with the same mind and heart of a human being but if programs are created and provided instructions in a similar fashion as human logic, they can certainly enhance decisions of people.

In a similar fashion to HCI&IM, HCSS focuses on bridging the gap between human reasoning and computational logic patterns (NITRD, N.D). This is not to be confused with Artificial Intelligence (AI), but is most certainly in a similar vein. If an information system can be programmed in such a way that it has a considerable amount of data and a skilled decision making tree from which to draw information, it can provide data with greater confidence than rote programmatic instruction sets. The purpose of improving HCSS is to provide government and private industries with more situation-aware systems that aid in (and sometimes perform) decisions with said information (NITRD, N.D). If research of these technologies is managed well, the US can increase the capabilities of mission critical systems and keep an edge over other nations.

Intel’s co-founder, Gordon Moore, when observing the world of semi-conductors and technology, determined that hardware capabilities of computer systems can be expected to double in complexity every two years (Geelan, 2008).

If one simply reads articles regarding computer science breakthroughs from even a few short years ago, it is easy to see that Moore's predictions turned out to be true. With each iteration of an operating system that is launched or with each new sequel released to popular computer games, the requirements for computer hardware and software increase. High End Computing (HEC) or High-Performance Computing (HPC) is the NITRD component which focuses on understanding these areas.

By continuing to focus federal attention and funding on HEC systems, the government and US research institutions are able to maintain a competitive edge over other nations when it comes to the raw processing power available in technology. The success of almost all of the NITRD research areas can be correlated with the power of the machines that can be used for these initiatives (Denzel, Li, Walker, & Jin, 2008). This places paramount importance on the success of HEC systems in maintaining the vitality of the other fields. For instance, Big Data processing is only as fast and capable as the systems used to process it. A lower powered machine is less likely to respond well in high-availability BD environments. Similarly, if an emergency worker is to use advanced HCI&IM technologies to make decisions, it follows that more powerful systems are likely to increase response time. If a HCSS tool is expected to make a rational decision based off any number of variables, it is logical that higher processing power of the decision systems would be beneficial. In essence, HEC truly is of vital importance to support advancing technologies across all fields and the US needs to prioritize its research on such projects.

As the technology advances, the need to produce quality software and enhance productivity also advances. NITRD has placed considerable research importance on Software Design and Productivity (SDP). As examined above, developers strive to find better and more efficient ways to enhance interaction between computers and humans. The increased demand for quality software has also generated demand for developers to be more efficient at software creation (Carver & Turoff, 2007). Software development lifecycles, rapid software development processes, and needs for increased quality of US software products are of special importance to NITRD. It is already clear that the manpower needed to engineer these next generation solutions is limited in the US (Kramer, 2011, pp. 9-10).

Despite this fact, the country is still capable of improving software development and finding even better ways to enhance productivity of the workforce.

By improving the processes and procedures used in development and training the next generation workforce in these methods, the USA can enhance its capabilities in production of quality software. Research needs to continue to focus on the implementation of newer and better processes, reusable code, and logical methodologies in software production (Benioff & Lazowska, 2005, pp. 5-6). Productivity and software functions are interconnected, as the quality and intuitiveness of software increases, so will the productivity boosts afforded by newer and better software applications. When the workforce of the USA is more productive, this offers numerous benefits to the quality of life of its information workers and improves the nation’s standing on the global stage. This concept leads in to the final area of focus for research and design – the social and economic impacts of technology on the workforce (SEW).

When the USA became involved in World War II, the workforce of the country had an astounding impact on US victory. The fundamental changes in the manufacturing field created a high demand for workers and the country happily obliged. Americans, especially women, quickly learned new skills and processes to aid in the war efforts (Zinni & Koltz, 2009, p. 27). This fundamental change in the ‘way things are’ not only aided efforts of the country but also added to the patriotic spirit of the American people. Those who learned new skills during the war found themselves gainfully employed after the war was over and the entire country benefitted from it.

It could be posited that the USA is on the verge of a new war, a cyberwar, which will require new skills in order for the country to compete. If history is any lesson, the workforce is going to require fundamental changes if they are to attain new skills needed to participate but the workers are few. The country is massively larger, more complicated, more disconnected from itself than ever before so it stands to reason that the country may not evolve in the same way as it did during WWII. This potential challenge is the focus of the NITRD initiatives regarding the social and economic impacts of technology and the workforce (SEW).

The country needs a wealth of knowledge workers with skillsets ranging from simple data entry all the way up to engineering of complex technology solutions.

Very few companies offer positions in the digital age that do not involve at least basic computer knowledge. Furthermore, the amount of technology used in even the most basic positions in the US workforce requires more computer knowledge than in previous generations (Benioff & Lazowska, 2005, p. 18). It would seem reasonable that a generation with ubiquitous access to technology would naturally produce more technically minded professionals but much of the workforce (especially in lower social castes) still lack many critical skills that the workforce demands. Conversely, some of the professionals in the modern workforce have become so intertwined with technology they use that it hampers their social capabilities otherwise (Mitchell, 2013). The new workforce does not originate from the same world as the aging (and often managerial) workforce already in the workplace and the potential for clashes to arise is ever-present.

If the government wishes to prepare the new workforce and support the merging of the 'old' workforce, there is great knowledge to be gained from social and economic research. NITRD wishes to engage in research that will help the country understand what impacts technology has on all walks of life. None of the other areas considered within NITRD's framework can be sufficient if the workforce is not prepared to rise to the challenge. By prioritizing research to understand how technology impacts the society in which the workforce lives, the government can take a more active approach in preparing for the new war.

By prioritizing research and design not only as it relates to the NITRD initiatives but as it relates to the country as a whole, the US stands a much better chance at returning to its former leadership glory. But these changes are not going to occur on their own. The country needs new leaders who can take up the mantle of leadership and adapt to this new world (Zinni & Koltz, 2009, pp. 41-42). The country also needs the assistance of its government to help usher in these changes and it is to this area that the conversation now turns.

5. The Hand that Leads You

Throughout this document, the importance of the government involvement in completing the security picture has been addressed but not fully expressed. Regardless of the political ideals one may hold or their personal opinions on the purpose of the government, the success of the country's future is quite dependent on the government's involvement.

The government is not only one of the biggest customers of American industry; it is also one of the greatest sources of funding. No matter how great an idea or technology may be it cannot go beyond an idea without at least some amount of financial support. Some ideas may be terrific in concept but without application they are useless. To this end, the government may offer a use case for technology that was otherwise untested or unproven (O'Neil, 2011).

Federal agencies have already made considerable progress in fostering the relationships both nationally and internationally that will be catalysts for improving security. From the groundwork laid out by PDD 63 to the Homeland Security Act, the leaders of the country are striving to improve security in all fronts. By using partnerships such as InfraGard between the FBI and the organizations that maintain critical US infrastructure, both parties are seeking to improve national security (Infragard, 2012). The implementation of Multi-State Information Sharing and Analysis Centers (MS-ISACs) has improved the communication between government and local organizations in the fields of cybersecurity and others. The National Security Administration (NSA) funds many classified and unclassified projects across a variety of businesses in many different sectors of the US economy (University of Maryland University Colelge, 2012). It is clear that the government plays a critical role in the adoption and sustainment of technology.

Although the federal government has been under considerable scrutiny by the media in recent years for spending and budgeting issues, there are still many funding sources available for new technologies and even for workforce education. The National Security Fund (NSF) offers financial assistance for American students who wish to pursue academic study in fields that support national security. The NSA offers funding through Cooperative Research and Development Agreements (CRADAs) for technology and research in a wide variety of technology disciplines (University of Maryland University Colelge, 2012). The Department of Defense and the military branches it represents offer contracts across a wide array of industries in hopes of developing bigger and better technologies than the enemies of the USA. These contracts offer financial support to industry and create millions of jobs nationwide - all in an effort to improve national security and build the economy.

As the USA continues to rebuild its empire for the digital age, it is going to need more complex technologies.

It will require more hardware and software to meet the needs of the new front in cyberspace. This demand means that the government will continue to push for better and more powerful technology. It will continue to set the standard for technology and drive the markets to support its needs and the needs of those that support it. This synergy of technological supply and demand is one of the many reasons why the government has a critical part to play in the future of cybersecurity. Therefore, the hand that leads the country is also the hand that is likely to direct the technological landscape. Failure to acknowledge the importance of government trends will ultimately lead to failure to prepare for the next cyberwar.

6. Summary and Conclusion

The field of cybersecurity continues to grow and change with every minute and so do the threats to the security of the USA. Many new technologies have become available in the past few years that can greatly improve efficiency and control in the enterprise and the government. Remote agent technologies can be used to improve the management and security of enterprise infrastructure and provide cost saving measures at the same time. Digital forensics will continue to become more and more vital to the security of the enterprise while maintaining scalability. In order to improve the efficiency of digital forensics, the enterprise may wish to consider the use of real-time and remote technologies which can both proactively monitor systems and respond to security incidents.

If the nation wishes to reclaim its position as a world leader in the digital economy, it must improve its capabilities in many technology fields. The Networking and Information Technology Research and Development program (NITRD) of the federal government has established priorities for research and design including Big Data, Human-Computer Interaction and Information Management, High-Confidence Software and Systems, High-End Computing, Software Development & Productivity, and Social and Economic Impacts of Technology in the workforce as top research priorities. Each of these elements is vital to the security and strength of the national economy, causing the majority of funding and research for the foreseeable future to be focused on these measures. By encouraging the development of these fields and the improvement of the STEM workforce, the government is attempting to position America at the forefront of the new digital era.

Additionally, the government itself plays a critical role in driving the market to pursue new technologies and developments. By the establishment of government projects, federal funded contracts, and public-private partnerships, the leadership of the country is actively supporting its own demands. As an offshoot of these endeavors, the country continues to revolutionize its industries and build world class solutions to compete on a global scale.

In conclusion, the demand for improved cybersecurity will require shared collaboration across all industries within the country and with the federal government. In time, these collaborations can potentially restore faith in the ability of America to lead the world as it has before. The country has made great strides in such measures as the use of remote management technologies, real-time forensic analysis, and by prioritizing research and design but the government needs to continually increase their focus on supporting these technologies if it hopes to succeed.

References

Adelstein, F. (2006). Live Forensics: Diagnosing Your System Without Killing It First. *Communications of the ACM, 49*(2), 64-66.

Agrawal, D., Das, S., & El Abbadi, A. (2011). *Big Data and Cloud Computing: Current State and Future Opportunities.* University of California, Santa Barbara, Department of Computer Science. Santa Barbara: Department of Computer Science, University of California Santa Barbara.

Barker, W. C. (2011). E-Government Security Issues and Measures. In H. Bidgoli, *Custom Textbook for CSEC620* (pp. 96-107). Hoboken: John Wiley & Sons Publishing.

Benioff, M. R., & Lazowska, E. D. (2005). *Cyber Security: A Crisis of Prioritization.* Arlington: President's Information Technology Advisory Committee.

Brusil, P. J. (2009). Medical Records Protection. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook Volume 2* (5th ed., pp. 71.1-71.35). Hoboken: Wiley and Sons Publishing.

Caballero, A. (2009). Information Security Essentials for IT Managers: Protecting Mission-Critical Systems. In J. R. Vacca, *Computer and Information Security Handbook* (pp. 225-258). Burlington: Elsevier.

Carver, L., & Turoff, M. (2007, March). Human-Computer Interaction: THe Human and Computer as a Team in Emergency Management Information Systems. *Communications of the ACM, 50*(3), 33-38.

Casey, E. (2011). Cybercrime Law a United States Perspective. In E. Casey, *Digital Evidence and Computer Crime* (pp. 85-121). Waltham: Elsevier.

Casey, E. (2011). Handling a Digital Crime Scene. In E. Casey, *Digital Evidence and Cyber Crime* (pp. 227-254). Waltham: Elsevier.

Denzel, W. E., Li, J., Walker, P., & Jin, Y. (2008). *A Framework for End-to-end Simulation of High-performance Computing Systems.* Marseille: SIMUTools.

Geelan, J. (2008, May 1). *Moore's Law: "We See No End in Sight", says Intel's Pat Gelsinger*. Retrieved February 23, 2014, from JDJ: http://java.sys-con.com/node/557154

Hockenson, L. (2013, March 25). *8 remote access tools to speed up your business*. Retrieved February 20, 2014, from The Next Web: http://thenextweb.com/insider/2013/03/25/remote-access/#!wC5DU

Infragard. (2012, February 18). *About InfraGard*. Retrieved from InfraGard: a collaboration for infrastructure protection: http://www.infragardmembers.org/index.php?option=com_content&view=article&id=51&Itemid=57

Ismail, A., Hajjar, M., & Hajjar, H. (2008). Remote Administration Tools: A Comparative Study. *Journal of Theoretical and Applied Information Technology, 4*(2), 140-148.

Kramer, F. D. (2011). Cyberpower and National Security. In F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyberpower and National Security* (pp. 3-23). Dulles: Potomac Books.

Kuehl, D. T. (2011). From Cyberspace to Cyberpower: Defining the Problem. In F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyberpower and National Security* (pp. 24-43). Dulles: Potomac Books.

Mitchell, A. (2013, August 15). *The Rise of the Millennial Workforce*. Retrieved February 23, 2014, from Wired: http://www.wired.com/insights/2013/08/the-rise-of-the-millennial-workforce/

Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to Computer Forensics and Investigations.* Boston: Course Technologies.

NITRD. (N.D). *High Confidence Software and Systems*. Retrieved February 22, 2014, from NITRD: http://www.nitrd.gov/nitrdgroups/index.php?title=High_Confidence_Software_and_Systems_Coordinating_Group_(HCSS_CG)#title

O'Neil, W. D. (2011). Cyberspace and Infrastructure. In F. D. Kramer, S. H. Starr, & L. K. Wentz, *Cyberpower and National Security* (pp. 113-146). Dulles: Potomac Books.

Orebaugh, A. (2006). Proactive Forensics. *Journal of Digital Forensic Practice*, 37-41. doi:10.1080/15567280600626411

Peng, L., Chen, W., Xie, D., Gao, Y., & Liang, C. (2013). Dynamically Real-time Anomaly Detection Algorithm with Immune Negative Selection. *Applied Mathematics and Science, 7*(3), 1157-1163.

Prowse, D. L. (2012). *CompTIA Security+ SYO-301 Certification Guide.* Indianapolis: Pearson Certification.

Richardson, T., Stafford-Fraser, Q., Wood, K. R., & Hopper, A. (1998, January-February). Virtual Network Computing. *IEE Internet Computing*, 33-38.

Salah, K., Alcaraz-Calero, J. M., Zeadally, S., Al-Mulla, S., & Alzaabi, M. (2013, January/February). Using Cloud Computing to Implement a Security Overlay Network. *IEEE Computer and Reliability Societies*, 44-53.

Spates, M. (2011, October 24). *How to make the web touchable: developing for a tablet interface*. Retrieved February 22, 2014, from Venture Beat: http://venturebeat.com/2011/10/24/developing-for-tablet-nui/

Street, J., Nabors, K., & Baskin, B. (2010). *Dissecting the Hack: The F0rbidd3n Network.* Burlington: Elsevier.

Trcek, D., Abie, H., Skomedal, Å., & Starc, I. (2010). Advanced Framework for Digital Forensic Technologies and Procedures. *Journal of Forensic Sciences, 55*(6), 1471-1480. doi:10.1111/j.1556-4029.2010.01528.x

Ullmer, B., & Ishii, H. (2000). Emerging frameworks for tangible user interfaces. *IBM Systems Journal, 39*(3 & 4), 915-931.

University of Maryland University Colelge. (2012, January 1). *Module 3: The Future of Cybersecurity Technologies.* Retrieved February 21, 2014, from University of Maryland University College: http://tychousa3.umuc.edu/cgi-bin/id/FlashSubmit/fs_link.pl?class=1402:CSEC670:9041&fs_project_id=508&xload&cType=wbc&tmpl=CSECfixed&moduleSelected=csec670_03

Virtue, T. (2009). U.S. Legal and Regulatory Security Issues. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook* (pp. 64.1-64.15). Hoboken: John Wiley & Sons.

Zinni, T., & Koltz, T. (2009). *Leading the Charge: Leadership Lessons from the Battlefield to the Boardroom.* New York: Palgrave Macmillan.