ICIT | Institute for Critical Infrastructure Technology

America is Under Siege:
Now is the Time for NASA to Unleash Gryphon-X

Authors:

James Scott, Sr Fellow at the Institute for Critical Infrastructure Technology

Drew Spaniel, Visiting Scholar, Carnegie Mellon University

Introduction:

Bureaucracy is the primary vulnerability that diminishes the cybersecurity capabilities of NASA and other federal agencies, and facilitates the devastating breaches that plague the nation. The siloed and protectionist territories ruled by inter-organizational politics result in a maximum exposed attack surface left vulnerable to exploitation by legions of hyper-evolved adversaries who possess endless agendas and who independently attack along an infinite number of vectors. Until now, state and well equipped mercenary actors dominated cyberspace's battlefield, but the recent claims of Anonsec, hactivists, and ransomware distributors demonstrate that even mundane attackers such as script kiddies, who lack technical sophistication and resources, can still barter on dark web forums for the exploits and user credentials necessary to compromise an organization and capture the information and media attention desired for their cause. NASA has been the pinnacle of innovation for over half a century; however, the prestigious position that once made NASA the envy of the technological world is rapidly diminishing due to the cancerous chaos incubating within the bureaucratic silos of the agency.

The vigorous 'all hands on deck' approach being used by America's adversaries seems to have been lost in the chaos and hierarchy power-plays that define America's agency communities. The ideas that sparked the innovation that put men on the moon are now snuffed out by political agendas spewed forth by NASA HQ's executive betters. The reality is, our Nation's virtually unprotected critical infrastructure is getting annihilated by sophisticated and not so sophisticated actors who use technology and virtual anonymity to infiltrate, surveil, and exfiltrate the interworkings of our most critical systems. Sadly, the one agency with the innovative intellectual capital needed to render solutions sits on its hands as it turns down one cybersecurity initiative after another meant to inject bleeding edge layered defenses into our dilapidated critical infrastructure technologies.

One such initiative that has received heavy HQ inquiries from the Senate and Congress is the Gryphon X project by Ames Research, a NASA campus located in the Silicon Valley. Set in the heart of the world's technology epicenter, this proposal, which targets cybersecurity defense solutions within our critical infrastructure with absolute surgical precision, has fallen into HQ's bureaucratic black hole without so much as the approval to socialize the concept among federal stakeholders on the Hill. As NASA literally reaches past the moon with its planned projects and missions, it desperately needs the Gryphon-X initiative to ensure mission assurance and to prevent loss of life and critical systems. It is the responsibility of the media and the public to motivate NASA HQ to approve the program for the sake of national cybersecurity.

The Threat to the Nation:

Make no mistake, America is at war, the American people are subject to exploitation by a vast and nebulous storm of adversaries, and Gryphon-X, a viable solutions capable of shifting the tide, is withheld in bureaucratic limbo within NASA. The cyber threat landscape can be aptly visualized as a complex battle between a seemingly infinite number of adversarial factions, possessing varying tactical and technological sophistication, and the besieged defenses of every organization in the world.

Some organizations are plagued by a vast uncoordinated horde of unsophisticated attackers. These script kiddies, hactivists, and nefarious employees have enough knowledge and resources to be dangerous, but they often lack the capability to individually cause catastrophic impacts. Picture them as a savage horde comprised of a vast number of separate nomadic tribes. Their weapons are primitive and their tactics are undisciplined. They are threatening predominantly due to their numerical advantage. While most of these attackers will be stopped by a vigilant security system, occasionally one or more might breach the defenses and infiltrate the network to steal some valuable asset or to wreak havoc within. Unsophisticated threat actors tend to be motivated by primitive desires such as fame, fortune, and causing destruction.

Recently, one group targeted NASA in hopes of accomplishing all three. In our February 2016 bulletin, ICIT analyzed a hacktivist group called Anonsec, who managed to infiltrate NASA cyber defenses due to outdated systems, undiscovered vulnerabilities, and negligent cyber-culture. Gryphon-X is designed to address all of these flaws within NASA.

On January 31, 2016, Anonsec contacted the Guardian and Wikileaks with data supposedly exfiltrated from NASA servers. Neither outlet published the information or responded for interview because they had profound respect for NASA and they doubted that such an unheard of group of script kiddies had actually compromised an organization that everyone expected to be more cyber diligent. The following day, Anonsec contacted journalist Mikael Thalen to publish their activity. The group subsequently published their own "zine" entitled "Op NASA Drones" that is modeled after a traditional security whitepaper. Overall, Anonsec released around 250 GB of data, though the size varies depending on where it is downloaded from because some sources uploaded it with different compression and some nefarious sources laced it with malware. The "safe" copies of the data contain 631 aircraft and radar videos, 2134 flight logs, and the contact information (work title, work phone number, etc.) of 2414 NASA personnel. All of the data released appears to have been publically available. The fact that many media outlets printed and propagated the incorrect claims that Anonsec had hijacked a drone should indicate to NASA HQ that the nation expected better of them. Otherwise, the story would not have been so sensational.

In actuality, NASA's cybersecurity has been in drastic need of reinforcement for years. In late 2013-2014, roughly seven members of Anonsec purchased a foothold into NASA's

network from two Chinese hackers. The exact cost of the foothold was not disclosed, but context clues in the IRC chat logs suggest that the price was not meager. Anonsec paid in compromised Bitcoin and other digital currency accounts. The foothold was a backdoor that remained after the Gozi virus compromised NASA systems between 2010 and 2013. The unsophisticated Anonsec members purchased the foothold because they believed that NASA was hiding Chemtrail data and that NASA was reducing the significance of global warming in media reports. With all of the unfounded conspiracy theories relevant to the significant work that NASA accomplishes, the administration should expect crazy hactivists to attempt to infiltrate the network or compromise systems. The demonstration that the administration did not adequately reinforce the network or promote initiatives like Gryphon-X is an indicator of negligence.

When Anonsec finally got around to accessing the network, they found their initial options limited. They could only access a bare minimum of commands from a least privileged account and the compromised server had the latest updates. Attempts to spear phish root credentials failed. However, the attackers soon acquired and utilized a symlink, which had an exploit to move further into the network. The exploit had been previously reported in cybersecurity communities because it had been used by the Mauritania Attacker, the leader of the AnonGhost team. If NASA had a cybersecurity fusion center, such as the one included in Gryphon-X, the systems would have been patched against the exploit and the attackers would not have been able to move further into the network. Anonsec navigated through a few systems and across a few networks thanks to the poor user credentials of a single employee named Eric Jensen, which were sniffed from a server. NASA internal security systems did not detect Anonsec's navigation through the network because the networks are not governed by a centralized security solution such as the one that would be provided by Gryphon-X. Over a few months, the group was able to access systems at the Glenn Research Center, Goddard Space Flight Center, and Dryden Flight Research Center; however, none of the systems compromised contained valuable information. Anonsec used Jenson's credentials to remain on a server for over a month before they discovered three 2TB WD My Book World Edition external hard drives connected to a network. The backup drives held drone flight record data, which had already been made available to the public. On a different system, Anonsec tried to conduct a man-in-the-middle attack and replace a file that contained the coordinates for the upcoming Global Hawk drone flight. They intended to alter the coordinates to misdirect and potentially crash the drone. Had they been successful, NASA would have lost a $222.7 million drone and, depending on where it crashed, lives could have been at risk. Thankfully, their access was denied and NASA was alerted to their presence on the network. Within 48 hours, the attackers could no longer access the network. None of their backdoors worked, they no longer received exfiltrated data, and their attack was over. Anonsec was not the first script kiddie group to successfully target NASA. Though specific details are not publically available, in darknet communities, as indicated in the first pages of the "zine", NASA is considered a meager and soft target that every kiddie worth his purchased scripts can infiltrate. NASA needs to change this opinion or attacks from script kiddies and more sophisticated attackers are likely to increase. Gryphon-X is a

powerful solution which would help NASA accomplish that mission, but for some reason, NASA HQ has left it sitting at their feet.

Organizations are also subject to the strategic attacks of resourced and sophisticated adversaries. These actors are less numerous, but their efforts are far more devastating. Sophisticated attackers launch sustained and coordinated campaigns that rely on informed decisions and deadly weapons. Instead of a rampaging horde, they arrive at a fortified position with trained personnel and complex weapons capable of either punching a hole through stalwart defenses or facilitating an unseen invasion and coup within the target's perimeter. Most organizations are simultaneously plagued by both unsophisticated and sophisticated attackers. The former continuously probes for weaknesses and stresses the resources. The latter either use the former as an additional weapon or use them as a distraction to the incumbent invasion. Sophisticated adversaries are motivated by more complicated agendas. One adversary may wish to steal NASA's intellectual property. Another might wish to diminish its reputation by leaking the personal information of its employees, thereby reducing its ability to retain talented personnel or acquire new talent. Yet another variety, might attempt to crash a shuttle at the site, commandeer a drone and crash it into a federal building, or prevent NASA from accomplishing its missions for a variety of political motivations. Gryphon-X would assure NASA's mission even more here than in the case of unsophisticated attacks. As described later, Gryphon-X has a fusion center capable of collecting data on applicable threats and integrating that data into preventative solutions.

The United States needs these preventative solutions against advanced persistent threats. Consider, the Black Energy group, a state-sponsored Russian advanced persistent threat group that has targeted systems of value to the Russian Federation or its military operations since 2008. The malware developed by the group was used in the 2008 cyber-physical attacks in Georgia. On December 23, 2015, Black Energy demonstrated that it could use its malware to deliver a component capable of disabling ICS, SCADA, and other industrial systems when it shut down a Ukrainian power grid for a few hours. The malware is delivered by traditional spear-phishing campaigns, but it can spread through other vectors and it can spread itself through infected networks. Given the history of using this particular malware in cyber-physical operations in the past, it is likely that the new capability will be used to facilitate such warfare in the future. The United States is not prepared for a cyber-physical war. If an enemy country shut off emergency systems and power grids across California for example, and then invaded, the United States may be taken unaware. Even if Black Energy is not directed against the United States, other malware will follow its form. Russia may not be willing to attack America at the moment, but can the same be said for North Korea, ISIS, or numerous mentally ill individuals on our own soil? Gryphon-X contains the fusion center, virtualization environment, and cyber-physical capabilities needed to analyze, prepare, and prevent threats like these from harming the nation, its organizations, or its people.

Our Antiquated Strategy and Defenses:

Organizations defend themselves from cyber adversaries in one of two ways. Either they invest in a "silver bullet" solution analogous to a large, thick wall, to deter enemy attack or they depend upon layers of defenses in the hopes of trapping invaders or whittling away the enemy's resources. The former strategy is utterly ineffective. Single source cybersecurity solutions are a charlatan's market. The products are prone to failure because a single vulnerability in the utility leaves the entire system vulnerable. The latter strategy is likewise, no longer entirely sufficient. Enemies have consistently adapted faster to the cyber landscape than organizations, evolved past defensive strategies, and outmaneuvered organizational defenses. The defense in depth model is the relic of a bygone time in cybersecurity. Information security professionals cling to it because no platform, like Gryphon-X, exists to develop and test a new model and solutions. Presently, discussions of compromise are no longer hypothetical predictions; instead, they are estimations of the future. For the moment, the battle for cyberspace is lost; however, the war can still be won.

NASA and every other organization in the public and private sphere requires a new approach to combatting cyber threats. Organizations, like NASA, operate complex networks across multiple facilities with limited governance and insight. Their response to cyber threats and full-fledged incidents is hindered by their lack of knowledge about their systems and their lack of training in realistic scenarios. These new solutions have not been investigated because under siege is not the optimal time to test new systems and stratagem. Organizations believe it better to use a failed defense in depth solution to slow and deter attackers than to try a new model only to open the network to a starving horde if the solution fails. If NASA HQ approves the initiative, Gryphon-X would enable organizations to defeat adversarial advances by providing the much needed applied cyber-physical environment in which comprehensive preclusive cybersecurity solutions and strategies can be researched, developed, tested, and evaluated and in which personnel can be trained in the application and response of these solutions.

Why NASA?

War is not about the strength of the forces controlled or the indomitability of defenses. A resourceful, persistent, or lucky adversary will always be able to outmaneuver a sitting target. Resisting compromise depends upon the intellect of defenders to develop agile and adaptive strategies that protect critical assets according to their value. With the right ideas and the right preparation, a miniscule force can defend itself indefinitely from any number of threats. At an ICIT meeting, a NASA representative said that "NASA does not have a monopoly on intellect." However, NASA does contain many of the most intelligent, most innovative, and most qualified personnel in the world. From an idealistic perspective, a single infallible leader would develop an impenetrable defensive strategy. NASA, in their vast wisdom as an innovative leader, has realistically out-thought idealism and in doing so, they have demonstrated that they should take a

leadership role in repairing national cybersecurity. They realize that a truly exceptional leader, invites the ideas of other great minds and facilitates the aggregation of those ideas and the needs of their providers into applicable solutions. Gryphon-X is the manifestation of this leadership.

NASA is comprised of Mission and Institutional networks that connect their critical infrastructure, systems, and applications. NASA, and every other agency and organization, has taken steps to secure its assets, only to discover that despite adherence to industry best practices, its systems are still vulnerable to cyberattacks because under the current cybersecurity solutions, no organization can address all security weaknesses in its network faster than attackers can discover and exploit the vulnerability. In response, Gryphon-X was developed to mitigate the risk to the network and preclude cybersecurity incidents through the facilitation of the next generation of cybersecurity solutions by proactively collaborating with the broader security community in academia, across the government, in other sectors, and in commercial entities.

Gryphon-X: The Solution That America Needs:

Adversaries are outmaneuvering modern cybersecurity defenses because organizations are relying on antiquated and underwhelming hardware and software solutions to protect critical assets. As a result, American organizations and citizens are being exploited by cyber attackers so frequently that most (especially those in the public sector who were victims of Anthem, OPM, etc.) are desensitized to the loss of their information. They have utterly accepted defeat at the hands of the adversary and many are doing absolutely nothing to change that vicious cycle for other victims. The brilliant minds at NASA Ames Research Center are not among the defeated. They saw how vulnerable America had become after the exploitation by adversaries had pushed victims to their knees. In response, NASA Ames Research Center developed the solution, Gryphon-X, to get American organizations in the public, private, and academic spheres back on their feet and into the war against adversaries unknown.

Gryphon-X is a NASA-wide Cybersecurity Fusion and Training Center facilitated and managed by the Ames Research Center in Silicon Valley California. The main approach to Gryphon-X is to manage security risk across NASA's critical infrastructure and to improve the resiliency of its networks. The implementation of the advanced technologies, facilities, and practices associated with the program will mitigate the cyber risks posed to NASA's extensive list of mission programs and projects. Currently, cyber threats to NASA's projects and missions can degrade, disrupt, or destroy mission critical assets. NASA Ames is offering to facilitate, and lead the development and execution of a holistic, mission assurance focused cyber vulnerability mitigation strategy that ensures network integrity across the plethora of missions, research projects, and programs under NASA's jurisdiction. Ames Research Center is uniquely qualified to assume this responsibility due to their geographic location in the Silicon Valley, their technological competencies, and their cross center, intergovernmental, academic, and commercial partnerships. NASA as an entire organization needs to explore and understand how current, new, and potential cyber threats can impact their critical assets and infrastructure. Ames

Research Center is offering a collaborative and holistic cybersecurity solution that will allow NASA to ensure its Mission. Without a solution like Gryphon-X, it is only a matter of time before some nefarious hacker jeopardizes expensive mission critical assets or threatens lives. What would be the impact to NASA's reputation and plans for the future if a hacker exploited a vulnerability in the software of a space launch system or crew capsule? How many lives might be lost if a satellite fell from the sky? How many different ways could an adversary utilize the army of unmanned autonomous systems that NASA develops? Lives, reputation, and the future of NASA are already at stake because all of these attacks are currently possible. The only reason that they have not occurred is that an adversary has not dedicated sufficient time, energy, and other resources to those targets. Gryphon-X would preclude those incidents and ensure the integrity of other important missions at NASA's core.

Gryphon-X is not limited in form or function like Cert's Stepfwd (which is predominantly used for workforce training) or INL's environment (which focuses on helping a limited few in limited ways). It is neither a certificate based organization nor a regulatory body. Gryphon-X is the collaborative solution that the public and private sector desperately need. The Cybersecurity Fusion and Training Center has a distinct purpose and, if approved, it will have the available resources to fulfill the objectives at the foundation of the initiative. Gryphon-X is, by design, a cyber-physical environment. The initiative includes both classified and unclassified facilities and infrastructure focused on performing applied cybersecurity training, research, development, testing, and evaluation on cyber systems. Gryphon-X aims to provide a collaborative environment that focuses on the security, stability, and performance of the critical infrastructure and cyber-physical systems upon which the federal government, private organizations, academic institutions, and military agencies depend. NASA personnel will work with affiliated partners in the specified organizations to optimize the potential of the pooled talent and infrastructure for the greater good of all parties involved. The objectives of improving the security, stability, and performance of assets will be addressed through the applied research, development, and enhancement of commercially available cyber tools and solutions in environments particular to the realistic attack surface. These solutions will be used to identify critical security deficiencies in NASA and other organizations to mitigate risk before attackers have the opportunity to exploit a vulnerability. Through the collaboration, Gryphon-X will be an expansive training environment for cybersecurity issues, technology, and processes with the goal of improving the cybersecurity posture of NASA, other federal agencies, and at other organizations across the nation. The Cyber Security Fusion and Training Center will facilitate the implementation of the security solutions and technologies developed across the 16 critical infrastructure sectors, which will improve the national cybersecurity defensive posture and facilitate a national discussion of cybersecurity.

The first capability of Gryphon-X is the physical facility, a Cyber Solutions and Training Center, located in the heart of innovation- the Silicon Valley. The campus will host classified and unclassified divisions capable of meeting the needs of any organization. The bleeding-edge

infrastructure will be capable of supporting the advanced applied cybersecurity research, development, testing, and evaluation characteristics of the program. This infrastructure is necessary to support NASA's mission operations as well as to explore the potential of experimental and emerging technologies. A dedicated facility is also important because it provides a centralized location for partners to collaborate and share information through the fusion center. The space can accommodate larger and more expansive efforts, such as experimentation on autonomous systems, without infringing on the areas required for other NASA projects. Embedded systems, otherwise known as cyber-physical systems, are characterized by the introduction of computer based sensors in a network that controls physical processes. Last year, researchers demonstrated that regular software infused cars were subject to devastating cyber-attacks. Since then, many other researchers have proven that other models are also susceptible to compromise. Many of NASA's current and future missions utilize more complex embedded systems, which are indefinitely vulnerable to cyber exploitation and are inevitably the next adversarial target. Autonomous vehicles are entirely dependent on vulnerable code. Attackers have not consistently targeted these systems because unmanned autonomous systems are not ubiquitous enough to profitably target. If the projects reach fruition and enter the market, without the adoption of Gryphon-X at NASA, then attackers will have no trouble jeopardizing the lives of those who adopt the technology. Devices that depend on the internet-of-things, such as robotic personal assistants (Watson, Amazon Echo, etc.), home security systems, and other devices are also at risk. Gryphon-X's facility would provide the physical laboratory space and the virtual environment necessary to test and secure these devices before they enter the market and attackers exploit them to cause physical harm, financial loss, or to steal information about the owners.

The fusion center of Gryphon-X would provide a much needed cybersecurity information sharing and integration nexus. Too often in cybersecurity information is siloed in individual firms, agencies, or sectors. Even among the information security community, research firms fail to collaborate and release differing accounts of threats or profile threats according to different names, tools, techniques, and procedures. The lack of standardized and aggregated information results in a plethora of under informed or misinformed audiences, who are ill-equipped to protect their networks. Since profiling adversaries is currently made difficult due to the dispersal of relevant data, anticipating the behavior of adversaries, for any meaningful amount of time, is next to impossible. Under the current conditions, threats strike, adapt, and evolve, before security researchers have time to discover the incident and develop a solution. Gryphon-X would alter those conditions. Information gathered in the fusion center can be integrated into working models of adversarial tools, techniques, and procedures. Indicators of compromise from victim systems can be paired with knowledge of exfiltrated information and profiles of the victim organization to predict where the adversary might strike next. Then those potential targets can be notified and trained to respond to the threat. In this manner, Gryphon-X aims to redefine the contested battlefield to provide defending organizations with the advantage of time and anticipation. Cybersecurity incidents will no longer be characterized solely by incident response;

instead, some incidents will be described by their efforts to premeditate and confound the adversary's attempts to compromise the networks. Aggregated reconnaissance on adversarial groups may provide the evidence necessary to definitively prove attribution of criminal and nation state threat actors. The theory of broken windows suggests that as a region becomes subject to an unanswered behavior, say breaking the windows of building with rocks, more individuals are likely to participate in that activity until a resounding initiative deters the behavior with actionable consequences. As more information floods into the fusion center and as more adversaries are profiled, the community will become better informed and better able to respond to the threats. Consequently, less individuals (knowledgeable grey-hat hackers, teenagers, etc.) will participate in the behavior and after enough momentum is generated, they will even act to deter negative activity. In this manner, the information security community can use information as a weapon to defend our system and recruit talented personnel from adversarial endeavors, without considerable changes to standard incident response procedures.

Gryphon-X would also feature a virtual and physical advanced cybersecurity training and educational institute. Humans are currently the weakest component of every organization. Technologically advanced organization and the Federal Government are the most affected because their intelligent and talented personnel are not accustomed to considering the cybersecurity ramifications of their actions within an organization. The current training and awareness endeavors across the nation have at the very best (and likely an overly optimistic estimate) an 85 percent effectiveness rate. This means that at least 15 out of every 100 employees do not retain the training necessary to not make the mistakes that put organizations at risk, such as clicking on a spear-phishing email. The Gryphon X institute plans to develop a novel and comprehensive curriculum based on teaching cybersecurity to those with a STEM background. The lessons will be available at the tangible institute and from a virtual platform. Courses will likely be provided synchronously and asynchronously as needed. The availability and impact of the development and delivery of a STEM based cybersecurity curriculum to personnel across the nation, is not to be underestimated. The cybersecurity field struggles with attracting objective, intelligent talent from the STEM discipline who possess the capabilities to experiment and analyze within an objective, constructive framework. These personnel, and even the currently non-technical cybersecurity personnel trained with the curriculum, will revolutionize the thought and procedure within the field. For instance, instead of two distinct personnel, say a programmer and an engineer, attempting to virtualize an asset, a single well-trained engineer, recruited into cybersecurity and trained with the curriculum, can virtualize the asset and emulate the real world capabilities and weaknesses of the device.

The Gryphon-X infrastructure would support a virtual, cloud based, simulation environment. The virtual "cyber range" will facilitate the research, development, testing, and evaluation of cybersecurity solutions under realistic conditions and according to the actual threat environment of the organization. This will be made possible by an extensive catalogue of virtualized physical systems. Essentially, the Gryphon-X systems would support emulated

versions of any current and outdated hardware or software network asset, complete with its real-world security flaws. In the environment, researchers can perform accurate penetration testing without harming the device or compromising their own network. Through this capability, participants can identify vulnerabilities and either develop mitigations (patches, mitigating controls, etc.) or monitor where adversaries are likely to enter the network. The worst time for an organization to test their defenses and strategy is during an incident. Gryphon-X would remediate that on-going cybersecurity deficit and enables organizations to develop and premeditate the best plan of defense, under a variety of conditions, before an attack ever occurs. In Gryphon-X, adversarial tactics can be simulated to gain insight into the attackers' tools, techniques, and procedures, or to train personnel to respond to a specific threat.

Conclusion:

Every bureaucratic silo erected, every politically motivated decision made by agenda driven protectionist executives, and every viable, forward thinking proposal ignored by an organization's leadership never to see the light of day, renders their own unique universe of vulnerabilities that adversaries will use to exploit our Nation's critical infrastructure. Legions of adversaries, possessing endless motivations, who attack along infinite variations and vectors are encircling the United States and the private sector who manage 90% of our Nation's critical infrastructure. This is not a time to sit on proposals that can have an optimal and profound impact on critical infrastructure resiliency. Gryphon X cannot be allowed to just be another proposal that got lost in NASA's notorious bureaucratic black hole. We must inject next generation evolution into the layers of NASA's project pipeline strategy in order to combat the compounding and hyper evolved threats. NASA has the opportunity to, once again, become a beacon that calls out to bleeding edge technology innovators to bring their technologies to be used and tested in the most evolved classified and non-classified simulation available. The time has come to unleash Gryphon X.

Sources:

ICIT:

http://icitech.org/icit-bulletin-anonsec/

NASA:

https://www.nasa.gov/centers/ames/home/

We Live Security:

http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/