Agile Methods For Improved Cyber Operations Planning

Dr. Jami M. Carroll
Unaffiliated, Somerset, MA, USA

[jcarroll@prisidian.com]

Abstract: Cyber Ranges provide an interactive simulated environment of hardware and software for simulation. This closed environment provides a safe and legal environment where cyber warfighters can refine their skills. They enable mock cyber mission rehearsal of operation playbooks. Simulated cyber capabilities in the cyber range parallel the intelligence, surveillance, and reconnaissance (ISR), Order of Battle (OOB), and battle damage assessment (BDA) in a closed, safe environment for experimentation. Scrum has been used in collegial cyber competitions with success because it has allowed Capture-the-Flag cyber games to create quicker simulations. Defense Innovation Units (DIUs) are using agile Scrum processes to numerous warfighting areas in order to make them more agile. This research argues that the agile software development processes could be used to optimize the planning and execution of offensive, defensive, and operation and maintenance (O&M) of cyber warfare simulations within cyber ranges. O&M can be done quicker, new exploitable modules can be includer more rapidly, and the capability can be reconstituted to the appropriate skill level for the next set of trainees quicker. The White team as maintainers of the networks, systems, applications and cyber tools select the CVE exploits and spend an enormous amount of time installing and configuring these capabilities for the next set of trainees. Quite often, there are different skill levels which require multiple builds and the ability to refresh the cyber range with varying levels of cyber trainee complexity. This requirement to restore the cyber range quickly with a variety of builds, varying levels of difficulty, and ensure the experiential learning is maximized with the best availability lends to agile methods such as Scrum could lend to improvements with cyber operations. This research will illustrate how a cyber range could leverage agile Scrum processes to provide an improved cyber range environment quicker and with more capabilities.

Keywords: Cyber Range, Cyber Security, War Game, Agile Methods, Scrum

1. Introduction

Disclaimer: All statements of fact, opinion or analysis expressed are those of the author. The views and opinions expressed herein by the author do not represent the official policies or positions of the United States (U.S.) Department of Defense (DoD), U.S. Navy, or other agencies or departments of the U.S. government and are solely representative of the views of the author. This does not constitute an official release of DoD or Navy information.

This study will examine how Agile Methods like Scrum can be applied to Cyber Ranges to significantly improve the offensive and defensive cybersecurity skills of the red and blue teams while providing a more responsive cyber range for the white team to manage (Vykopal, Jan et al., 2017). National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) describes cyber ranges as cloud-based environments allowing educators, government, industry, and the military to provide offensive and defensive cyber security training to participants to expand their skills (NIST NICE, 2018). The U.S. Cyber Range indicates that these simulated representations of networks, systems, applications and cyber tools that provides performance-based learning and assessment; develop cyber teamwork; enable real-time feedback to be given in an environment that simulates real-world scenarios while operating in a safe environment where new tools, techniques, and procedures can be applied (U.S. Cyber Range, n.d.). Red team are the offensive cyber attackers trying to breach the networks, systems, and applications using techniques ranging from hacktivism to nation-state level attacks. Blue team are the defensive cyber defenders trying to protect the networks, systems, and applications. The White team designs the cyber war game, injects stimuli such as scripted attacks, simulated intelligence reports, and tasking orders requiring red and white team responses (Sullivan et al., 2018). Lectures and labs alone provide a limited facet of how the cyber warfighter will need to respond. In actual war, there are military Operation Plan (OPLAN) which lays out how they will fight the battle, including the cyber battle. A key element is Intelligence Preparation of the Operational Environment (IPOE) which will focus on developing course of actions (COAs) to support the warfighter. This IPOE will include cyber elements related to Intelligence, Surveillance, and Reconnaissance (ISR), Order of Battle (OOB), and the Battle Damage Assessment (BDA) as they are executed (Couretas, Jerry, 2022). Cyber Range warfighters will use these battle scenarios to develop Tactics, Techniques and Procedures (TTP) that can lead to improved tradecraft in handling real world responses when not in the cyber range. Tradecraft in cyber warfare requires extraordinary secrecy, deception, stealth and strategy to hide the exploit while using intelligence, planning and operations to achieve the attack before the defender can patch, reconfigure, or use other countermeasures to thwart the attack requiring the attacker to change their cyber operations attack plans (Gartzke & Lindsay, 2017). Because the operation of the cyber range is so important to the learners within the constrained training period, it is critical that the Cyber Range is constantly available for use. Unlike a typical enterprise information technology (IT) system, the cyber range is

constantly going through an exercise lifecycle covering the exercise's development, dry run, execution, evaluation, and repetition as well as coming up with new scenarios as vignettes within the OPLAN (Vykopal, Jan et al., 2017). In 2022, MITRE published 25,068 new vulnerabilities in the Common Vulnerability Exposure (CVE) database – an increase of 24.3% beyond 2021 (Jacobs et al., 2023). The White team as maintainers of the networks, systems, applications and cyber tools select the CVE exploits and spend an enormous amount of time installing and configuring these capabilities for the next set of trainees. Quite often, there are different skill levels which require multiple builds and the ability to refresh the cyber range with varying levels of cyber trainee complexity. This requirement to restore the cyber range quickly with a variety of builds, varying levels of difficulty, and ensure the experiential learning is maximized with the best availability lends to agile methods such as Scrum could lend to improvements with cyber operations. The primary research question is: How can agile software development processes like scrum be applied to improve Cyber Range operations and learning? It is anticipated that the results of this study could be used to enhance all Cyber Ranges and that this foundational work may help U.S. Service/Agencies, Allies, and Partners.

2. The Evolution of Cyber Ranges

The first cyber ranges were largely classified Department of Defense (DoD) built to test cyber as weapons much like weapon testing grounds used for the first nuclear weapons. These early DoD cyber ranges were used by cleared government and contractors much like going to the gun range. Because a DoD clearance, classified networks and need-to-know / need-to-use were involved, very few users had access to these cyber ranges. The Michigan Cyber Range is considered one of the first non-government cyber ranges created in 2012 after discussion with leadership at the White House and U.S. Department of Homeland Security (DHS) by the Michigan state cybersecurity team. Michigan focused on two goals with their Michigan Cyber Range: 1) workforce development and skills training and 2) development by academic and university organizations to replicate the U.S. Military Academy at West Point Information Warfare lab (IWAR) (Lohrmann, Daniel, 2018).

Another expansion towards the needs for cyber ranges evolved as a result of the National Security Agency (NSA) creating the Centers of Academic Excellence (CAE) in Information Assurance Education degree program created in 1999. The University of Texas at San Antonio (UTSA) is credited with starting the first U.S. collegial cyber competitions in the southwest in 2005 to extend these NSA degree programs with applied learning. In 2010, the U.S. House passed Resolution 1244 recognizing the importance of cybersecurity education programs and the need for cyber ranges and cyber exercises and the need for a National Collegiate Cyber Defense Competition (NCCDC) to promoted cybersecurity curriculums (Schafer, Joseph H., Morrell, Chris and Blaine, Ray, 2022).

As these NCCDCs started identifying their learning outcomes, they realized there were three main groups of learning. One group, the defenders, were responsible for designing, configuring, and protecting the network and its resources. A second group, the attackers, were responsible for conducting the vulnerability assessment / penetration testing of the network infrastructure, databases, mail servers and Web servers. A third group was responsible for the day-to-day operation and maintenance of this environment and the ability to quickly restore it after exercise completion or worse yet, the addition of new attack/defend capabilities, or even catastrophic failure resulting from attacks. NCCDCs came to realize that maintaining an excellent learning environment with a high degree of availability for the learning teams was a daunting task.

Cyber ranges train cyber warfighters against cyberthreats by criminals, state actors, and non-actors. In order to provide the necessary offensive and defensive cybersecurity skills, cyber ranges provide a critical capability for active learning where theory is supplemented with application (Vykopal, Jan et al., 2017). Lectures and labs alone only provide one side of the learning and lack the true impact gained from analyzing how each side affected the attack. The combination of combining offensive and defensive training allows interactions between the offensive and defensive players inside a safe and legal closed environment that closely mirrors real world operations. (Ferguson, Bernard, Anne Tall, and Denise Olsen, 2014; National Initiative for Cybersecurity Education (NICE), 2018). These virtualized environments have Web servers, databases, multi-tiered architecture, and network infrastructures that are similar to real-world operations (Vykopal, Jan et al., 2017).

Vulnerability assessment is the initial finding of potential vulnerabilities that may be exploitable while penetration testing is the actual exploitation of the vulnerability found; the actual exploitation of the system crosses the line of potentially illegal acts similar to espionage that occur in a cyber range. The sequence of steps such as footprinting, fingerprinting, enumeration, research, escalation, repeat visits, and covering of tracks cover the steps involved in vulnerability assessment through penetration testing to achieve the attack while maintaining stealth. Figure 1 illustrates the typical steps used in vulnerability and penetration testing of systems.

Vulnerability assessment involved the collection of information through footprinting, fingerprinting, enumerating, and then researching the possible attack vectors. Once the vulnerability phase is completed, the penetration tester develops a list of possible attack vectors based on either ease of attack, effects achieved by the attack, or when simulating a hacker or state actor, acquiring a particular data element. Acquiring a particular data element in the NCCDC is sometimes referred to a "capturing the flag" (Carroll, 2017).

	Common Approaches	Description	Comments
Vulnerability Assessment	Footprinting	Where do the IP addresses/systems show up?	• Reconnaissance (active (scanning) or passive (sniffing) • External – DNS and external-facing systems (nslookup, whois, dig, SamSpade, NMAP, & Zone Transfer) • Internal – SNMP, Unix, Windows, LDAP, SMTP, & NMAP) *Note: Approach is slightly different if coming from inside the network than from outside the network*
Vulnerability Assessment	Fingerprinting	What are the ports and services for the OSs and Applications?	Fingerprinting (scanner with OS recognition)
Vulnerability Assessment	Enumeration	What version of a service exists? (Example – banner grabbing of a web server or mail server)	Enumeration, potential vulnerabilities
Vulnerability Assessment	Research	Common Vulnerability Database (CVE.mitre.org); National Vulnerability Database (http://nvd.nist.gov/);Open Source Vulnerability Database (www.osvdb.org)	
Penetration Test	Escalation	Privilege escalation, Denial of Service, Man in the Middle	Obtain access
Penetration Test	Repeat visits	Backdoors - Hackers do this - Pen Testers simulate unless authorized to perform destructive testing (DoD) - Computer Network Attack (CNA)/Computer Network Exploitation (CNE) may do this when authorized	Maintain Access
Penetration Test	Covering tracks	Log zappers, log stoppers - Hackers do this - Pen Testers simulate unless authorized to perform destructive testing (DoD) - Computer Network Attack (CNA)/Computer Network Exploitation (CNE) may do this when authorized	Erase evidence

Figure 1. Typical Steps Used in Vulnerability and Penetration Testing of Systems

3. Cyber Wargaming: A Venue for Mission Rehearsal

War games attempt to simulate military operations against an opposing force in what might be similar conditions. The concept of war games goes back to Sun Tzu's 5th century BC era and the term was first coined in 1824. The advantage of the wargaming experience for military leaders is acquiring a lot of practical experience without "real-world penalties" (Sullivan et al., 2018, p. 92). Cyber wargaming simulates the "red team" as the attackers, the "blue team" as the defenders, and the "white team" as the designers and executors of the war game (Sullivan, D.T., et al., 2018). The white team designs the war game with a pre-planned state and objectives for the red and blue team to achieve. Many of these cyber ranges have added gamification objectives where quantitative points, levels, and leaderboards are gained by the team based on their offensive or defensive efforts (Diakoumakos, 2021). Gamification has increased student interest / enthusiasm because the game scenarios very closely emulate real-world situations within virtualized environments in cyber ranges with practical training gained through experiential learning at educational institutions. With a lack of cyber warfighters and an ever increasing number and sophistication of attacks, a continuous stream of cybersecurity education can be offered (Jelo, M. and Helebrandt, P., 2022).

Cyber Ranges enable mock cyber mission rehearsal of operation playbooks (Vykopal, Jan, 2017). Mission Rehearsal Exercises (MREs) are conducted prior to many major operations. Prior to the infamous Operation Neptune Spear which led to the raid on Osama bin Ladin's complex and his death, numerous mockup MREs were conducted to simulate the operation prior to execution (Gratch, Jonathan and Marsella, Stacy, 2003; Christensen, Gitte Højstrup, April 2017; Kiras, James D., 2017).

For the military, these isolated environments enable cyber missions to be rehearsed, and capabilities evaluated. Much like in actual war, there is the equivalent of a military Operation Plan (OPLAN) which lays out how they will fight the cyber battle based on hypothetical scenarios, military objectives, and military doctrine for the forces being used. Cyber OPLANs will have wargaming segments supporting cyber intelligence surveillance reconnaissance (ISR), creating a cyber-oriented Order of Battle (OOB), and a cyber intelligence battle damage assessment (BDA) that are broke into smaller sections of ISR, OOB, and BDA that are handled by cyber teams

from a variety of military and government entities with different skill sets (Blasch, Erik, and Micheline Bélanger, 2016).

In order to keep pace with technology, since the early 2002s, quite a bit of the U.S.'s Command, Control, Communications, Computers and Intelligence (C4I) systems are built with standard Commercial-Off-the-Shelf (COTS) hardware, software, and firmware and far less Government-Off-the-Shelf (GOTS) hardware, software, and firmware. This allows technology insertion to happen quicker and at a significantly decreased cost. Another advantage is that many of the standard information technology capabilities found in industry are also directly used in government C4I systems (Huskey, T.W., 2007). This allows new technology in industry to be used in cyber ranges and provide a similar environment to what cyber offensive and defensive teams can be trained within the cyber range (Couretas, J.M., 2022).

4. Agile Software Development Processes

Since cyber ranges must create multiple simulated representations of networks, systems, applications and cyber tools based on: 1) varying student skill level of students being trained, 2) quickly restore these representations to a pristine environment for the next set of student, and 3) constantly adding new real-world vulnerabilities, DevSecOps could significantly improve how quickly cyber ranges could be setup. The quicker the White team can integrate new vulnerabilities and simulated injects, the closer to a real-world environment that the cyber range will take on. The White team can simulate simulated capabilities as models that allow attackers to create exploits while defenders can protect. Examples of these models include code injection attacks, denial-of-service (DoS) attacks, identity-based attack, insider threats, malware, phishing, spoofing and supply chain attacks. These models provide valuable learning opportunities for the Red team to perform exploits while the Blue team hardens their systems against these exploits. The counterbalance between the attackers and defenders leads to the development of TTP that is highly applicable to real-world operations. Agile methods using Scrum have made up to a fourfold improvement compared to non-Agile methods (Sutherland & Sutherland, 2014).

Traditional software development lifecycle (SDLC) approaches like the spiral or waterfall models can take several years to decades for complex systems. These traditional SDLC approaches often lack the design thinking & agile approaches to meet cutting edge capabilities (Pereira, J.C. and de FSM Russo, R., 2018). Worse yet, long development cycles can lead to endless requirement creep, unfulfilled system end state, cancelled program, and hardware refresh prior to delivery since the software evolves faster than the hardware (Giachetti, R.E. and Van Bossuyt, D.L., 2022). Iterative and incremental evolved between the 1950s and 1970s with many lightweight agile software approaches gaining maturity in the 1990s. The best of these agile approaches came together when the Agile Alliance developed the Agile Manifesto in 2001 (Fowler, M. and Highsmith, J., 2001).

Highsmith and Cockburn argued that software development metrics indicated that most software development using traditional software lifecycle development methodologies failed to satisfy the customers. The main reason it failed was because of a focus on conforming to a plan as the primary goal and satisfying the customers at time of delivery as a secondary goal. In addition, requirements, scope and the technology used was constantly changing throughout the projects period of performance -- this further meant that the final delivery to the customers was even further away from desired. The assumption under traditional software lifecycle development methodologies was that any variation from the originally devised plan would cause unacceptable errors which would further cause deviation from the initially designed plan (Highsmith, J. and Cockburn, A., 2001).

Agile software development processes outlined four tenets with the goal of improving software development and reliability while providing significantly better "customer value". These tenets desired the following outcomes: 1) focus on the individuals and their interactions as being more important than processes and tools; 2) develop working software that fulfilled its intended purpose over extensive documentation; 3) collaborate directly with customers over negotiation via contracts; and 4) respond to necessary changes to the software over following a hard development plan. The Agile Manifesto developed 12 principles focused on early-on and continuous software development that provided value-added software in less time and of a greater quality and reliability (Fowler, M. and Highsmith, J., 2001). Sutherland & Sutherland argued that Agile software development processes can help developers quadruple their software delivery when Agile is fully embraced (Sutherland, J., & Sutherland, J. J. (2014). Agile software development processes accepts that while errors can occur, they cannot be completely eliminated and rather than putting so much effort in eliminating rework, the approach should be to reduce costs associated with this rework, but continue to focus on software quality. Agile software development processes also accepted that it is important to continuously understand the customer's needs for

the software and accept requirements can change, but by staying continuously engaged with the customer throughout short one to four week periods of development in a sprint, the software was more likely to meet the customer's needs. In order for this to work, the most commonly used agile software development process, Scrum, focused on 15-minute daily Scrum team meetings and 30-minute comprehensive Scrum team reviews at the end of each one- to four-week Sprint cycle (Highsmith, J. and Cockburn, A., 2001).

Scrum is an agile project methodology approach that helps a team structure and manage their work in small increments called sprints where the Scrum team applies empirical processes to provide iterative capabilities by ensuring their processes are transparent, inspectable and adaptable as these new increments of change are required (Scrum Org, n.d.). The U.S. military has adopted Agile Processes outside of software development for a variety of warfighting use cases because it achieves results significantly faster than waterfall methodology approaches; the main reason is that Scrum is value-oriented vice Waterfall methodology being schedule-oriented. Uses outside of software development include reorganizing "command and control, quick reaction capabilities, rapid acquisition offices, and US force transformation" (Tomar, A.K., 2017, p. 11). Douglas claimed that Agile Multi-Domain Command and Control is leveraging agile processes to increase advances in how artificial intelligence (AI), autonomous systems, aircraft and nuclear weapons are so critical to military capabilities that Agile processes have been adapted to achieve best possible benefits (Douglas, O.C., 2020). The hardware design for the CubeSat Multi-Mission Bus Demonstration (MBD) project leveraged Agile processes (Huang, P.M. et al., 2012). A major multinational military aviation company uses Agile processes to develop their family of aircraft (Freitas et al., 2020). The Defense Innovation Units (DIUs) like NavalX are focusing on how to provide Agile processes to a variety of warfighting areas, where Scrum can be applied in a militaristic construct (NavalX, 2022). Some of the NCCDCs have started looking at leveraging Scrum in their cyber competition environment because of the operation and maintenance required by the White Team to be able to provide a ready environment for a continuous stream of NCCDC participant teams using their cyber range environment (Novak, H., 2013).

Figure 2 illustrates the Scrum Framework. The following describes the main blocks within the Scrum Framework (Scrum.org. 2023):

- The product backlog lists all functionalities, the requirement for the functionality, a short description of those functionalities. The product owner maintains this product backlog of all desired capabilities for the system. For a cyber range, this may include new capabilities that the offensive and defensive warfighters will get such as the latest technology, technology with known vulnerabilities (e.g. log4J), newer cyber tools being released, or application / operating system patches.
- Sprint planning is done by the product owner, development team, and Scrum Master. It identifies the capabilities that will be done during the one- to four-week sprint. Two hours per number of weeks is allocated to sprint planning. For a cyber range, this may include patching or upgrading software items that were too easy for the offensive warfighters to attack. For the defensive warfighters, it may be applying DoD or business preferred hardening techniques to make the component harder to attack.
- The Sprint backlog is what is being worked on during the one- to 4-week sprint. The Spring backlog must identify the "definition of done" for the capability under development – this becomes their mantra for success. Because these changes are being done in a development environment before pushed to a production environment where the offensive and defensive warfighters are wargaming, both development and production environments can be run simultaneously to allow continuous training events.
- The single Scrum team is a team of less than 10 people focused on development of the Sprint. They will meet daily for no more than 15 minutes to discuss the user story of what the capability is doing, what is and what is not working, and changes that must be done to accomplish the work.
- The Product Increment is the incremental / iterative increment of the product that is either useful or provides value to the product under development.
- The Sprint Review is attended by the product owner, Scrum Master, development team, and all stakeholders / customers / sponsors. It is used to demonstrate the working and tested Product Increment created during the Sprint. This meeting is timeboxed to no longer than one hour times each week of Sprint.
- The Sprint Retrospective is attended by the product owner, Scrum Master, and development team to talk about what went well and what did not go well. It is focused on continuous improvement. This meeting is timeboxed to no longer than one hour times each week of Sprint.

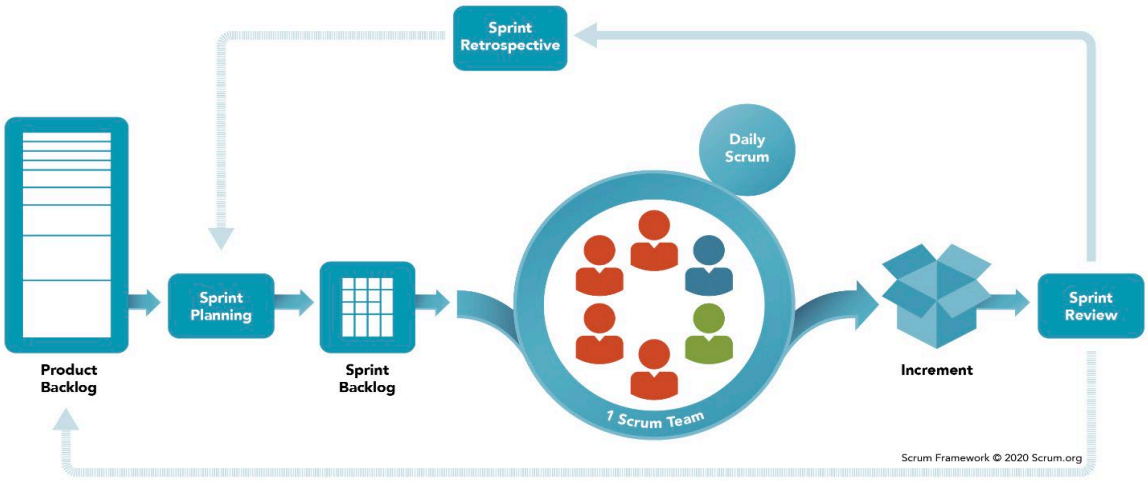

Figure 2. The Scrum Framework.

5. DevSecOps

Development, Security, and Operations (DevSecOps) is a combination of automation, platform and culture that is applied within an information technology (IT) lifecycle. DevSecOps allows rapid and frequent development cycles. Figure 3 illustrates a DevSecOps environment, there is Continuous Integration (CI) coupled with Continuous Deployment (CD) with a Blue Green Pipeline. At the far right, the current production capability is called the Blue Pipeline and represents the current cyber range configuration and referred to as "Current Version N". The next version of the cyber range configuration is called the Green Pipeline and referred to as "Current Version N + 1". The N + 1 version is the one that has received the Scrum Increment. Starting at the far left in Step 1, the Scrum Team is working on the Increment assigned in Sprint Backlog. As the Increment is being worked on, the code branch is put into a repository (e.g. Github) during step 2. During step 3, the code branch is pushed to the Static Application Security Tools (SAST) and Dynamic Application Security Tools (DAST) in step 4 for regression / security testing. If they pass all tests successfully, they are sent to step 5. If they do not pass all step 4 testing, they are sent back to step 1 for rework and continuation with the process. Once the code branch successfully gets to step 5, the software is staged for final acceptance / quality assurance testing. If it passes, it is sent to the N + 1, New Version as a future production release. A package / artifact manager releases the product to the Production environment when it is ready to be fielded.

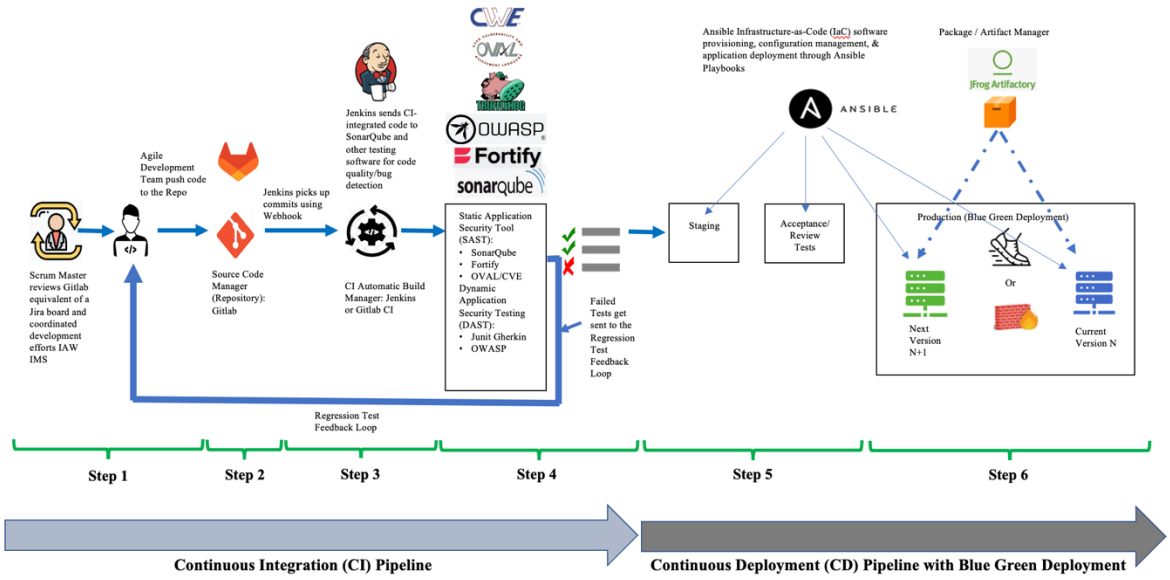

Figure 3. Development, Security, and Operations (DSO) environment

In a cyber range, offensive security testing often requires a complete re-installation or re-imaging of the systems after each training event because the systems have different parameters than when the cyber warfighters started their practice. This is required because software is broken, misconfigured, and services are modified during the penetration testing. Virtual Machine (VM) imaging is one of the best ways to restore the system to the original state before the next red and blue teams can start using them. Since the cyber range is always adding new features, providing timely patches, and security hardening the system, the DSO environment with Blue Green Deployment along with VM imaging allows the White Team an ability to maintain the current and next system for continuous availability of a cyber range suite for classes as they are needed.

6. Conclusion

This research argues that the agile software development processes, such as Scrum coupled with a DevSecOps could significantly optimize the planning and execution of cyber ranges. New capabilities that the offensive and defensive cyber warfighters will get such as the latest technology, technology with known vulnerabilities, newer cyber tools being released, or application / operating system patches could be managed via Scrum and pushed out via the Development, Security, and Operations (DevSecOps) environment extremely fast while providing an environment that allows for the next version to be quickly created and ready to be pushed out as a VM image. Having highly available systems that can quickly support mock cyber mission rehearsal of operation playbooks allows Cyber OPLANs with wargaming segments supporting cyber ISR, OOB, and BDA in a closed, safe environment that would allow cyber warfighters to get the best possible active learning environment.

References

Blasch, Erik, and Micheline Bélanger. "Agile battle management efficiency for command, control, communications, computers and intelligence (C4I)." In *Signal Processing, Sensor/Information Fusion, and Target Recognition XXV*, vol. 9842, pp. 248-258. SPIE, 2016.

Christensen, Gitte Højstrup. April 2017. Interdisciplinary Perspectives on Special Operations Forces. In *The 2016 Royal Danish Defence College (RDDC) Conference* (No. 2017). Royal Danish Defence College.

Couretas, J.M., 2022. Cyber ISR and Analysis. In *An Introduction to Cyber Analysis and Targeting* (pp. 91-118). Cham, Switzerland: Springer.

Diakoumakos, J., Chaskos, E., Kolokotronis, N. and Lepouras, G., 2021, July. Cyber-Range Federation and Cyber-Security Games: A Gamification Scoring Model. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 186-191). IEEE.

Douglas, O.C., 2020. Transforming DOD for Agile Multi-Domain Command and Control. *Joint Force Quarterly*, *97*, pp.83-90.

Fowler, M. and Highsmith, J., 2001. The Agile Manifesto. *Software Development*, *9*(8), pp. 28-35.

Freitas, F., Silva, F.J., Campilho, R.D.S.G., Pimentel, C. and Godina, R., 2020. Development of a suitable project management approach for projects with parallel planning and execution. *Procedia Manufacturing*, *51*, pp.1544-1550.

Gartzke, E. and Lindsay, J.R., 2017. Thermonuclear Cyberwar. *Journal of Cybersecurity*, *3*(1), pp.37-48.

Giachetti, R.E. and Van Bossuyt, D.L., 2022. Challenges of Adopting DevOps for the Combat Systems Development Environment. *Defense AR Journal*, *29*(1), pp.22-49.

Gratch, Jonathan and Marsella, Stacy, 2003. Fight the Way You Train: The Role and Limits of Emotions in Training for Combat. *Brown Journal World Affairs*, *10*, p.63.

Highsmith, J. and Cockburn, A., 2001. Agile Software Development: The business of Innovation. *Computer*, *34*(9), pp.120-127.

Huang, P.M., Knuth, A.A., Krueger, R.O. and Garrison-Darrin, M.A., 2012, May. Agile hardware and software systems engineering for critical military space applications. In *Sensors and Systems for Space Applications V* (Vol. 8385, pp. 104-112). SPIE.

Huskey, T.W., 2007. *Impacts and Consequences of Non-Standard COTS C4I System Acquisition Upon Associated Programs of Record*. Naval Postgraduate School, Monterey, CA.

Jacobs, J., Romanosky, S., Suciuo, O., Edwards, B. and Sarabi, A., 2023. Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights. *arXiv preprint arXiv:2302.14172*.

Jelo, M. and Helebrandt, P., 2022. Gamification of cyber ranges in cybersecurity education. In *2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA)* (pp. 280-285). IEEE.

Kiras, James D., 2017. "Risky Business": A Conceptual Inquiry of Special Operations and Risk. *Interdisciplinary Perspectives on*, p.142-164.

National Initiative for Cybersecurity Education (NICE). 2018, *Cyber Ranges*. Viewed December 13, 2022, https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf.

NavalX. 2022. Centers for Adaptive Warfighting: Agile Training for Warfighters. https://www.secnav.navy.mil/agility/Pages/caw.aspx.

Novak, H., Likarish, D. and Moore, E., 2013. Developing Cyber Competition Infrastructure Using the SCRUM Framework. In *Information Assurance and Security Education and Training* (pp. 20-31). Springer, Berlin, Heidelberg.

Pereira, J.C. and de FSM Russo, R., 2018. Design Thinking Integrated in Agile Software Development: A Systematic Literature Review. *Procedia computer science*, *138*, pp. 775-782.

Schafer, Joseph H., Morrell, Chris and Blaine, Ray, 2022. The IWAR Range+ 21 Years: Cyber Defense Education in 2022. *Military Cyber Affairs*, *5*(1), pp.1-13.

Scrum.org. n.d. What is Scrum. [https://www.scrum.org/learning-series/what-is-scrum].

Scrum.org. 2023. The Scrum Framework Poster. https://www.scrum.org/resources/scrum-framework-poster.

Sullivan, D.T., Colbert, E.J.M., Hoffman, B.E. and Kott, A., 2018. Best practices for designing and conducting cyber-physical-system war games. *Journal of Information Warfare*, *17*(3), pp. 92-105.

Sutherland, J., & Sutherland, J. J. (2014). *Scrum: The Art of Doing Twice the Work in Half the Time*. New York. Crown Business.

Tomar, A.K., 2017. *Study of Scrum Framework Usage in Non-Software Systems* (Doctoral dissertation, Massachusetts Institute of Technology).

U.S. Cyber Range. (n.d.) What is the U.S. Cyber Range? https://kb.uscyberrange.org/faq/us-what-is-cyber-range.html.

Vykopal, J., Vizváry, M., Oslejsek, R., Celeda, P. and Tovarnak, D., 2017, October. Lessons learned from complex hands-on defence exercises in a cyber range. In *2017 IEEE Frontiers in Education Conference (FIE)* (pp. 1-8). IEEE.