Paper
06

Winning in the Digital Frontier
Developing Cyber Targeters and Military Daring

Dr. Greg Austin
Adjunct Professor,
Australia China Relations Institute,
University of Technology Sydney, Australia

Abstract

The specialists needed most for winning battles in cyberspace are the targeters. Their role is a highly complex one: to discover and exploit vulnerabilities in adversary systems to disrupt or disable them while achieving cognitive or physical impacts on enemy forces. The corps of targeters must be highly trained and have considerable experience across many intelligence-related domains, including politics and psychology. The targeters must also exist in large enough numbers, with a high diversity of specializations to support operational goals. Their leaders must have the military daring and expertise needed to achieve operational outcomes based on their advice. The relationship between targeter and commander in cyberspace is potentially more significant than in any other field of operations, save for nuclear weapons. The development of a standing force of highly capable cyber targeters, supported by advanced processes for linking them with forward-deployed military commanders, is the main priority for success on the digital battlefield.

Introduction

In the development of cyber personnel for national security functions, including air power, no single role may be as important as that of targeter. This view has been expressly shared by two Chinese military specialists who see the role as the 'fundamental work in [a] cyberspace operational plan' (Zhang and Yao, 2015). The United States Air Force (USAF) also has strong advocates for the view that cyber targeting should be at the center of its strategy and development plans for full-spectrum cyberspace operations (Anderson, 2016).

These sentiments, although not often encountered in open-source discussions about cyber military operations, can be easily justified. Targeters can take on deeply complex tasks, breathtaking military ambition, and heavy responsibilities given evolving warfighting concepts. These concepts have been variously expressed over two decades. China's cyber forces have been tasked to undertake operations to 'paralyze the enemy's operational system-of-systems [... and] sabotage the enemy's war command system-of-systems' during the early stages of hostilities (Costello and McReynolds, 2018). U.S. leaders have talked about 'global strike in milliseconds' (Cartwright, 2009) or cyber options for all phases of operations (Cyber Command, 2015). The most ambitious U.S. concept has been to achieve 'penetration and then disintegration of an adversary's systems and decision-making, thereby defeating their offensive capabilities' (Pacific Command, 2020).

This article looks at what is needed to marry a cyber targeter's talent to the goal of system penetration and profound disabling effects that can defeat adversary kinetic capabilities. The discussion suggests that a long-standing orthodoxy on the limited value of cyber operations in war will, in time, be overcome by the realization of just how military daring and ambition can help realize the full potential of cyber warfare.

Cyber Targeters

Cyber targeters play a lead role in integrating cyber capabilities with other forces in political or military operations. In the CIA and the USAF, the targeter roles are highly demanding: to 'leverage the most advanced cyber tools, datasets, and methodologies to analyze all-source information' (CIA) to support targeting decisions in both offense and defense. Targeting decisions depend on a deep knowledge of adversary and domestic IT

Targeting decisions depend on a deep knowledge of adversary and domestic IT systems, operating procedures, capabilities, and military or strategic planning.

systems, operating procedures, capabilities, and military or strategic planning. The personal profile of these analysts usually involves an advanced degree in related technical sciences, expertise in a foreign language, and prior U.S. intelligence experience. The complexity of the cyber targeting mission is laid bare in the USAF (2021) doctrine on targeting. It set a clear expectation that target development for operational concepts and tasking orders should 'integrate specialized analysis in support of space, cyberspace, electromagnetic spectrum, and information operations'.

In cyber operations, targeting is a continuous process of investigation, planning, system penetration, attacks, damage assessment, follow-on exploitation, reprioritization, and re-attack. It depends on deep knowledge of and access to adversary systems. Unlike in kinetic operations, where, for example, much can be done using stand-off photo imagery of the target, in cyberspace, such analysis is dependent on maintaining engagement with and presence in adversary cyber systems. As an example, Figure 6.1 depicts the process of an example attack combining multiple frameworks, and may incorporate hundreds of sub-techniques and tools during mission execution.

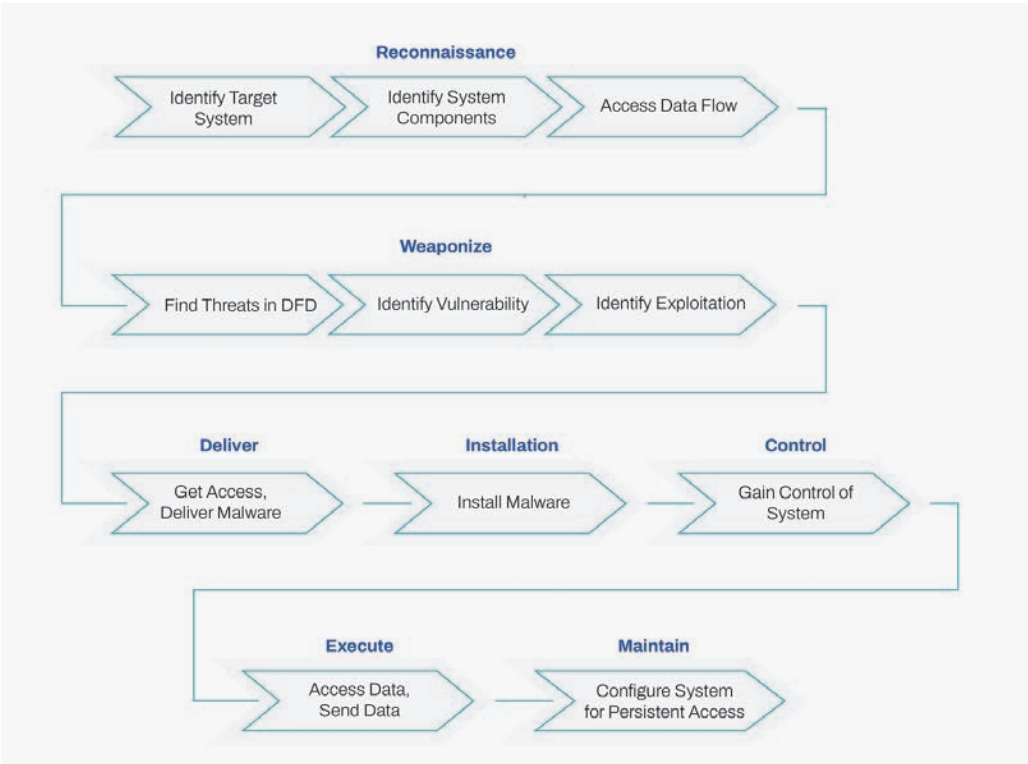

Figure 6.1: Example of Attack Combining Multiple Frameworks (adapted from Straub, 2020)

According to the USAF, cyber targeting is 'often more time-consuming' than kinetic operations because of the character of the domain (USAF, 2023). Planning must include consideration of 'significant second- and third-order effects' as well as deconfliction with intelligence agencies, policy departments, and (as circumstances dictate) allies. Targeters are also involved in cyber defense, in identifying vulnerabilities in mission-critical cyber terrain that may come under attack from adversaries. However, in official USAF doctrine, 'targeting' refers only to offensive cyber operations (USAF, 2023).

Cyber targeting functions need to be in place at the three levels of warfighting (strategic, operational, and tactical). In the U.S., Cyber Command works with unified combatant commanders (for example, the U.S. European Command) as the lead on strategic missions, such as attacking adversary command and control. USAF cyber personnel contribute to these strategic missions under assignment to Cyber Command, but the air force concentrates its cyber planning and targeting on operational and tactical missions.

The USAF began this process for targeter development at least in the 1990s, deploying cyber targeters to the 1999 NATO bombing campaign against the former Yugoslavia. The air force began to consolidate this in 2006 when it began setting up its own Cyber Command (Air Force, 2006), a move it suspended when the joint force Cyber Command was being established several years later.

USAF cyber capabilities remain under continuous review and development. For example, in 2024, a senior USAF officer, Lt. Gen. Leah Lauderback, deputy chief of staff for intelligence, surveillance, reconnaissance, and cyber effects operations, saw considerable opportunity to further develop tactical cyber operations in support of air superiority compared with their current relatively underdeveloped state (Pomerlau, 2024a). Key organizational elements of this (creation of a novel Cyberspace Wing and development of an operational concept for Cyber-Enabled Air Superiority) are not expected to mature until the 2025-27 timeframe. This timeframe will see recruitment and training of new cohorts of cyber targeters. An interesting insight into how the USAF has been responding to tactical needs in cyberspace targeting can be found in an analysis by one of its officers on incorporating cyber capabilities into USAF special operations (Kopecki, 2016).

The Central Intelligence Agency (CIA) openly advertises the role of cyber targeter and describes its heavy responsibilities as 'generate operational leads, drive successful operations' (CIA, undated). The United States Air Force (USAF) includes the role of targeting as a specific specialization in its intelligence musterings. At the same time, cyber targeters are provided to U.S. agencies and forces in seemingly large numbers by private sector firms, such as General Dynamics, BAE Systems, and Booz Hamilton, judging by the advertisements on U.S. job pages.

In 2022, the U.S. Department of Defense amended its doctrine on Joint Cyberspace Operations to give more attention to expeditionary action (operations involving the 'deployment of cyberspace

forces within the physical domains' (Pomerlau, 2023). This would have important implications for targeters, especially the potential imposition of new burdens for quickly coming up to speed with previously unanalyzed systems or relationships between those systems and other operational objects. In August 2024, the USAF revealed its plan to upgrade the level of cyber advice to the air force chief by splitting the functions of an existing Deputy Chief of Staff for intelligence and cyber into two different appointments, given the emerging significance of cyberspace operations and the need for specialists advice in that field (Pomerlau, 2024b).

Cyber Orthodoxies

There is a long-standing orthodoxy that offensive cyber operations can only have limited effect in military conflict. In 2009, Martin Libicki, one of the most respected scholars of cyber warfare, concluded in a report he wrote for the USAF that 'strategic cyberwar is unlikely to be decisive' and that 'operational cyberwar has an important niche role but only that' (Libicki, 2009). In 2012, Thomas Rid and Peter McBurney from King's College London made an important distinction between target-specific cyber weapons that may be high value in terms of effect and those of more general application that are of lower value in terms of effect (Rid and McBurney 2012, 6). They said there is a clear penalty involved in developing the high-value weapons which 'increase the resources, intelligence and time required for development and deployment' and which are 'likely to decrease the number of targets' and the 'political utility of cyber-weapons.

There is a long-standing orthodoxy that offensive cyber operations can only have limited effect in military conflict.

These assessments were sound at the time, but they must be interpreted against the definitions of 'cyber war' or 'cyber weapon that the authors used. In the Libicki case, his definition of cyber war was a narrow one (does not involve 'real' war, that is a physical one) (Libicki, 2009). Rid and McBurney define a cyber weapon somewhat narrowly as 'computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings'. At the same time, they suggest more research is needed into system-wide effects and that the very concept of cyber war is problematic.

In 2018, a U.S. study identified three strands of thought (more like stages of development) in the U.S. defense establishment (Paul et al., 2018). These strands were: 'sprinkleism' (meaning that little bits of information operations are okay and are usually an afterthought), total commitment to the potential of information operations through structure, resourcing, and integration, and a paradigm shift to full acceptance of and planning for outcomes where the information environment is the 'primary

determinant of those actions.' The report left little doubt of its view that, at the time, the DoD was stuck somewhere between 'sprinkleism' and total commitment to information operations and was falling well short of the paradigm shift those cyber capabilities appeared to offer.

Beginning in 2018, the U.S. armed forces became much more proactive in their approach to cyber operations in a way that might open up new potential for offensive action but which was, in essence, defensive. Cyber Command (2018) adopted a vision that the U.S. could gain and hold cyberspace superiority. The Pentagon separately moved to a strategy of persistent engagement in cyberspace operations, in which a major component was the concept of 'defend forward' (Department of Defense, 2018). It would involve new levels of defensive action, both in friendly and hostile networks, against adversary operations. These would remain below the threshold of armed conflict but would involve new levels of regular access by U.S. operators to adversary networks. This access would, in turn, better position U.S. forces for rapid transition to more wide-ranging offensive cyber operations.

These shifts helped lay the groundwork for more ambitious statements about the U.S. intent to paralyze its adversaries in cyberspace, such as the 2020 statement cited above aiming for the 'disintegration of an adversary's systems and decision-making.'

Fast forward to 2024, an academic study relying heavily on analysis of the Russia-Ukraine war reiterates the orthodoxy. It concludes that there is limited utility of cyber operations in war 'owing to an unsuitability for physical destruction, high risks of failure, high costs of complex [cyber] operations that are more likely to attain successful and destructive effects, and a dichotomy between the tempo of conventional and cyber operations leading to cross-domain integration difficulties' (Pedersen and Jacobsen, 2024).

On the other hand, however, they argue that there may be 'two narrow windows' for pursuing military utility. These are the prospects for 'cumulative strategic utility from 'targeting critical infrastructure and governments in a persistent barrage of less complex cyber operations; and by concentrating on operations at the outset of combat since 'cross-domain integration can be planned before warfighting commences'. The article identified organizational decisions and technical challenges as primary reasons for the lack of cross-domain cyber operations rather than fear of escalation or legal constraints.

As I have pointed out elsewhere (Austin, 2016), there are at least three critical dimensions of the policy problem presented by cyber warfighting that the assessments supporting the long-standing orthodoxy did not take into account:

- Radical technical advances in cyber weapons
- Changes in the political character of cyber weapons as countries accumulate entire cyber arsenals rather than an inchoate collection of unique single cyber weapons (attack packages)

- Changes in strategy as countries move away from conventional military practices to cyber-age strategies where information dominance and cyberspace superiority are considered possible.

Thus, over time, we should expect the conclusions by Libicki, Rid, and McBurney are likely to be less relevant. Indeed, Libicki (2017) provided a seminal article on the convergence between information warfare and cyber operations in which the last question was clearly answered in the affirmative, even though he did not frame it in quite that way.

Military daring

There is another critical angle. If an adversary's biggest military vulnerability is in its cyber systems for strategic command and control or in its cyber control of weapons systems and platforms, why would an adversary military commander not seek to attack such vulnerabilities? Should a military commander accept the long-standing orthodoxy or seek to test the limits? Does the commander want cyber targeters who say some missions can't be executed and are not cost-effective or targeters who can at least develop the attack options, no matter how difficult? Are the obstacles more organizational (issues of choice) rather than inherent in the technologies?

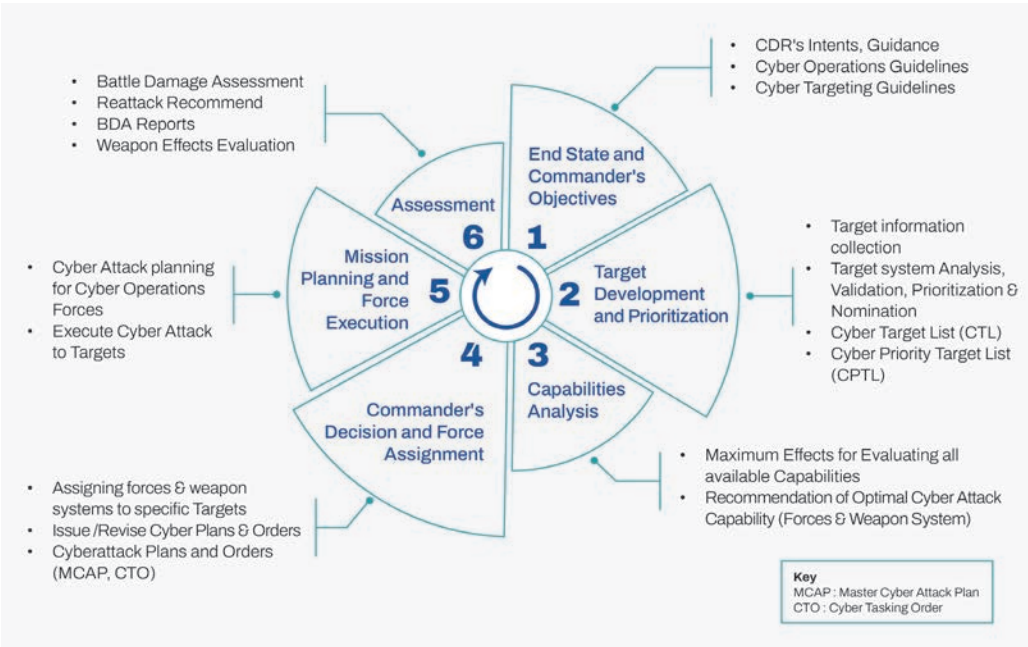

Figure 6.2: Cyber-Targeting Process (Kim et al., 2022)

Targeting in cyberspace can be very complex, especially where system effects are being pursued. Any given cyber targeting process, such as the one illustrated in Figure 6.2, will very often depend on a multi-vector intelligence collection effort in cyberspace over an extended period. Most of the analysis will be beyond the comprehension of military commanders who are not cyber specialists. The complexity at the technical level has been well laid out in a Korean study (Kim and Eom, 2016). According to the same study, there are additional political, social, cognitive, and institutional aspects of cyber capability that need to be analyzed and potentially targeted.

So, the combat commander intent on exploring offensive cyber options will likely need a large team of targeters with diverse specializations who are actively working the mission options over an extended period. A study of the Stuxnet worm estimated that various teams of specialists (up to 45 people) would have been engaged over two years or so to create the worm (de Falco, 2012). Stuxnet was used in an attack on an Iranian nuclear fuel plant that may have physically destroyed up to 1000 centrifuges (de Falco, 2012). This analysis concluded that 'Stuxnet differs from any other precedent worm because of its complexity, flexibility, potentiality, combination of features, multi-role performance and goal' (de Falco, 2012). It demonstrated that creative thinking could create previously unimagined cyber effects at scale.

Moreover, technologies favoring the feasibility of strategic-level offensive cyber operations have come into play over the past 15 years. High-performance computing, human-machine teaming, and artificial intelligence have shifted the ground under pre-existing orthodoxies about the limited value of cyber operations. As one study notes, 'AI and machine learning have already been used to improve the content of phishing e-mails, avoid spam-filters, and better map and systematize the collection of data on specific targets, which continues to be the foundation for most cyberattacks' (Jacobsen and Liebetrau, 2023). Targeters are now able to complete complex tasks needed for effective cyber attacks at the strategic level at far greater speed than fifteen years ago.

Conclusion

The keys to strategic effects in offensive cyber operations appear to lie more in military ambition, organization, and advance planning than in technological limitations. In wartime, the maximalist will be to paralyze or decapitate adversary decision-making while severely disrupting communications, command, and control. In setting these ambitions, military commanders will be entirely dependent on the creativity and knowledge of their cyber targeters. There is no certainty that they will be able to produce the effects being pursued. However, with the right caliber of targeters, organized and led for maximum impact, and rewarded accordingly, offensive cyber operations will almost certainly have notable strategic effects. There will, for now, be less likelihood that such effects can be decisive on the outcome of battles or war, but several countries are probably within reach of such capabilities.

REFERENCES

Anderson, S. (2016) Airpower Lessons for an Air Force Cyber-Power Targeting Theory. School of Advanced Air and Space Studies. Available from: https://media.defense.gov/2017/Nov/21/2001847267/-1/-1/0/DP_0023_ANDERSON_AIRPOWER_LESSONS.PDF

Austin, G. (2016) AUSTRALIA REARMED! Future Needs for Cyber-Enabled Warfare. ACCS Discussion, Paper 1. Available from: https://www.socialcyber.co/_files/ugd/15144d_6a1eb662e90e4c96beb5ccfa655cbc6a.pdf

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B. and Anderson, H. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. New York: Cornell University Press. Available from: https://arxiv.org/pdf/1802.07228

Cartwright, J. (2009). Presentation at the Center for International and Strategic Studies, June 4, 2009. The text is no longer available on the world wide web.

CIA. Undated. Cyber Targeter. Available from: https://www.cia.gov/careers/jobs/cyber-targeter/

Costello, J. and McReynolds, J. (2018). China's Strategic Support Force: A Force for a New Era. Washington, DC: National Defense University Press. Available from: https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf

Cyber Command. (2015). Beyond the Build: Delivering Outcomes through Cyberspace. Washington, DC: U.S. Department of Defence. Available from: https://nsarchive.gwu.edu/sites/default/files/documents/2692135/Document-27.pdf

Cyber Command. (2019). Achieve and Maintain Cyberspace Superiority. Washington, DC: U.S. Department of Defence. Available from: https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

De Falco, M. (2012). Stuxnet Facts Report. A Technical and Strategic Analysis. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Available from: https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

Department of Defense. (2018). Summary. 2018 Department of Defense Cyber Strategy. Washington, DC: Department of Defense. Available from: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf

Jacobsen, J.T. and Liebetrau, T. (2023) Artificial intelligence and military superiority: How the 'cyber-AI offensive-defensive arms race' affects the U.S. vision of the fully integrated battlefield. In F. Cristiano, Broeders, D., Delerue, F., Douzet, F. and Géry, A., (2023) Artificial Intelligence and International Conflict in Cyberspace, Issue 1, pp. 135-156

Kim, K.H. and Eom, J. (2016) Modeling of cyber target selection for effective acquisition of cyber weapon systems. International Journal of Security and Its Applications, 10(11), pp. 293-302. Available from: https://article.nadiapub.com/IJSIA/vol10_no11/24.pdf

Kim, K., Oh, S., Lee, D., Kang, J., Lee, J., & Shin, D. (2022). A Study on Cyber Target Importance Quantification and Ranking Algorithm. Applied Sciences, 12(4), 1833. https://doi.org/10.3390/app12041833

Kopecki, T. (2016). New Tools for a New Terrain: Air Force Support to Special Operations in the Cyber Environment. Maxwell Air Force Base: USAF Air Command and Staff College. Available from: https://apps.dtic.mil/sti/tr/pdf/AD1040710.pdf

Libicki, M. (2009). Cyber deterrence and Cyberwar, Santa Monica CA: Rand Corporation. Available from: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Libicki, M. (2017) The convergence of information warfare. Strategic Studies Quarterly 11.1, pp. 49-65

Lopez, C. (2006), Air Force leaders to discuss new 'Cyber Command' [Online] Air Force Print News. Available from: https://www.af.mil/News/Article-Display/Article/129517/air-force-leaders-to-discuss-new-cyber-command/

Pacific Command. (2020), Transforming the Joint Force: A Warfighting Concept for Great Power Competition [Online]. Available from: https://www.pacom.mil/Media/Speeches-Testimony/Article/2101115/transforming-the-joint-force-a-warfighting-concept-for-great-power-competition/

Paul. C., Clarke, C., Triezenberg, B., Manheim, D., and Wilson, B. (2018) Improving C2 and Situational Awareness for Operations in and Through the Information Environment. RAND. Available from: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2400/RR2489/RAND_RR2489.pdf

Pedersen, F. and Jacobsen, J. (2024) Narrow windows of opportunity: the limited utility of cyber operations in war. Journal of Cybersecurity. Volume 10, Issue 1. Available from: https://academic.oup.com/cybersecurity/article/10/1/tyae014/7727352?login=false

Pomerlau, M. (2023), New DOD doctrine officially outlines and defines 'expeditionary cyberspace operations' [Online]. Available from: https://defensescoop.com/2023/05/12/new-dod-doctrine-officially-outlines-and-defines-expeditionary-cyberspace-operations/

Pomerlau, M. (2024a), 'This is overdue'– Air Force creating tactical cyber capabilities to ensure air superiority [Online]. Available from: https://defensescoop.com/2024/05/23/air-force-creating-tactical-cyber-capabilities-ensure-air-superiority/

Pomerlau, M. (2024b), Air Force splitting up intelligence and cyber effects organization [Online]. Available from: https://defensescoop.com/2024/08/28/air-force-splitting-up-intelligence-cyber-effects-organization/

Rid, T. and McBurney, P. (2012). Cyber Weapons. RUSI Journal. February/March vol. 157 (1), pp.6–13 Available from: https://www.tandfonline.com/doi/epdf/10.1080/03071847.2012.664354

USAF. (2021). Air Force Doctrine Publication 3-60, Targeting. Washington, DC: U.S. Air Force. Available from: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf

USAF. (2023). Air Force Doctrine Publication 3-12, Cyberspace Operations. Available from: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf

Zhang, C. and Yao, Z., (2015). A game theoretic model of targeting in cyberspace [Online] IEEE. Available from: https://ieeexplore.ieee.org/document/7280218