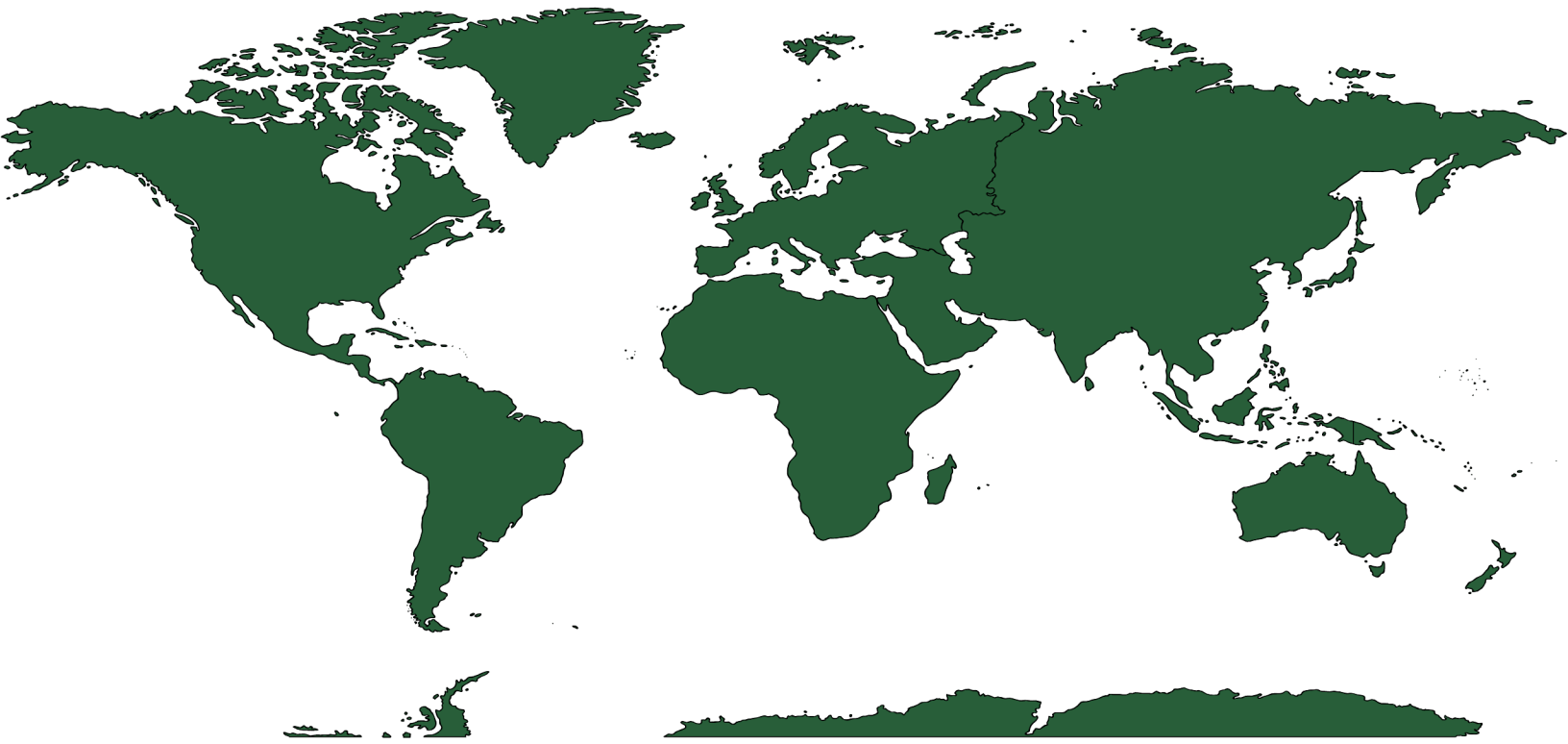
UTAH VALLEY UNIVERSITY
CENTER FOR NATIONAL SECURITY STUDIES

THE JOURNAL OF INTERNATIONAL SECURITY & STRATEGIC STUDIES

VOLUME XI - ISSUE I
SPRING 2026



The Journal of International Security and Strategic Studies

The Journal of International Security and Strategic Studies is published once annually—in the spring—and it is supported by the Center for National Security Studies (CNSS) at Utah Valley University (UVU). The JISSS publishes timely, insightful articles on critical international security matters, including topics relating to foreign affairs, intelligence, homeland security, terrorism, and US national defense. Submissions may be sent to the Editor-in-Chief at: CNSSJournal@uvu.edu.

The Center for National Security Studies

The CNSS at UVU was established in January 2016. The Center is the first of its kind in the State of Utah. The CNSS is a nonpartisan academic institution for the instruction, analysis, and discussion of issues related to the field of US national security. The mission of the CNSS is twofold: to promote an interdisciplinary academic environment on campus that critically examines both the theoretical and practical aspects of national security policy and practice; and to assist students in preparing for public and private sector national security careers through acquisition of subject matter expertise, analytical skills, and practical experience. The CNSS aims to provide students with the knowledge, skills, and opportunities needed to succeed in the growing national security sector.

Utah Valley University

UVU is a teaching institution that provides opportunity, promotes student success, and meets regional educational needs. UVU builds on a foundation of substantive scholarly and creative work to foster engaged learning. The university prepares professionally competent people of integrity who, as lifelong learners and leaders, serve as stewards of a globally interdependent community.

Volume XI Issue I
Spring 2026

CONTENTS

A Note From the Editor-in-Chief

Dear Readers,

It is with great honor that I present to you the Spring 2026 edition of the Journal of International Security & Strategic Studies. This journal is a collection of scholarly work from contributors across a wide range of academic and professional backgrounds, all engaging with critical issues relating to international security, strategy, defense, and global affairs. The articles presented in this edition reflect the complexity, and continued relevance of the field of international and strategic studies.

I would like to begin by thanking the contributors to this edition. Your academic rigor, revisions, depth of research, and commitment to quality scholarship are all clearly evident in your work. We sincerely appreciate your decision to submit your research to this journal, and we are grateful for the high caliber of scholarship we had the opportunity to review and publish.

Next, I would like to thank my editorial staff for their tireless efforts throughout this entire process. Your adaptability, professionalism, timeliness, and attention to detail were instrumental in bringing this publication together. The quality of your editing and the effort you dedicated to this journal did not go unnoticed, and I am sincerely grateful for your contributions.

I would also like to extend a special thank you to our faculty advisor, Professor Roberto Flores, for his continued guidance and support throughout this process. His experience in research and academia was invaluable during the development and publication of this edition. This journal would not have been possible without his leadership and mentorship.

Finally, I would like to thank you, the reader, for taking the time to engage with this publication. Your support and interest are the reason this journal exists. It is my hope that the articles in this edition will inspire new ideas, broaden perspectives, encourage meaningful discussion, and connect readers with important issues in the field of international and strategic studies.

Sincerely,
Josh Reid
Editor-in-Chief

A Brief Review of Multiple Image Encryption

Muhanned AL-Rawi

ABSTRACT

The technique known as multiple image encryption (MIE) offers efficiency and increased security over encrypting individual images by protecting multiple images at once. This method works especially well for applications involving large amounts of image data, like secure data storage, medical imaging, and remote sensing. Through the use of a unified cryptographic mechanism or a single encryption key, MIE can guarantee a uniform security framework for every image, increasing its resilience to breaches. It can further improve security by utilizing strategies like employing a single initialization vector and salt value. The literature review on multiple image encryption is presented in this paper.

Keywords: Multiple image encryption; literature review

1-Introduction

MIE is an advanced encryption strategy designed to handle the development of data, especially photographs used every day in most fields, and to protect multiple images at once rather than encrypting them at a time. This solution uses a unified cryptographic mechanism to manage images of different types. Therefore, MIE provides single protection that reduces the impact of breaches and is more complex than isolated protection of single images and reduces computational costs compared to the processing of each single image separately. Encryption is a way to ensure that all images are protected in a consistent security framework, allowing efficiency and better security[1].

Because it uses the correlations and interdependence between multiple images to increase encryption strength and security, MIE is necessary. In MIE, the attacker must decrypt all images at once, making it much more difficult to attack and hiding features that may otherwise be visible in individual images. The unified encryption operation used by MIE reduces the time required for encryption and decryption. It is therefore suitable for real-time applications such as live streaming. Using more than one image in a single operation reduces computational complexity and resource usage, especially for limited processing power or bandwidth. MIE techniques are very flexible to image types, formats, sizes, and dimensions and can be scaled quickly to fit large datasets[2].

[1] M. Meselhy, et.al.,"Multiple image encryption techniques: Strategies, challenges, and potential future directions,", Alexandria Engineering Journal, vol.125, pp.367-387, 2025.

[2] M. Meselhy, et.al.,"Multiple image encryption techniques: Strategies, challenges, and potential future directions,", Alexandria Engineering Journal, vol.125, pp.367-387, 2025.

1.1- Multiple image representation

Effective encryption, data integrity, and MIE performance depend on the structure and representation of images. Augmented Image Representation (AIR) and Stacked Image Representation (SIR) standard formats facilitate encryption when multiple images are prepared in a particular format [3].

Multiple images are combined into a single large image in the context of Augmented Image Representation (AIR). Using this technique, separate images can be arranged in a grid or side by side to form a single composite image. Within the larger image, each image maintains its original structure; however, for encryption purposes, the images are handled as a single, cohesive unit. The augmented image is then subjected to the encryption algorithm, which simplifies the process of managing several images separately. Fig.1 illustrates the general procedure for combining images in accordance with this AIR.

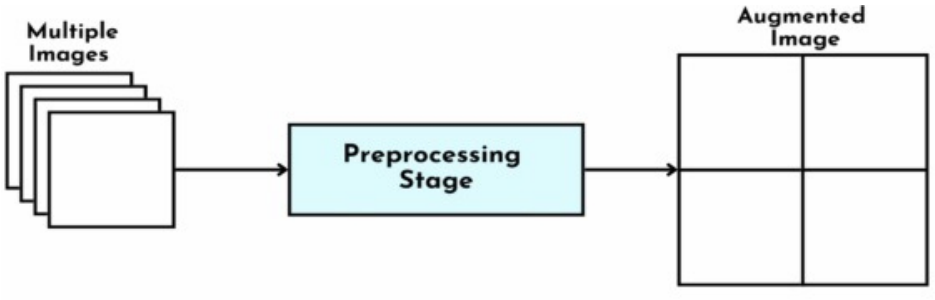


Fig. 1 Augmented image representation

A layered approach is used in stacked image representation (SIR), where images are stacked along a third dimension and arranged in layers to create a multidimensional structure, like a 3D array. The stacking procedure can be carried out spectrally, combining various channels or modalities, or spatially, stacking images one on top of the other (like a cube). Fig.2 illustrates the general procedure for combining images based on this SIR.

.

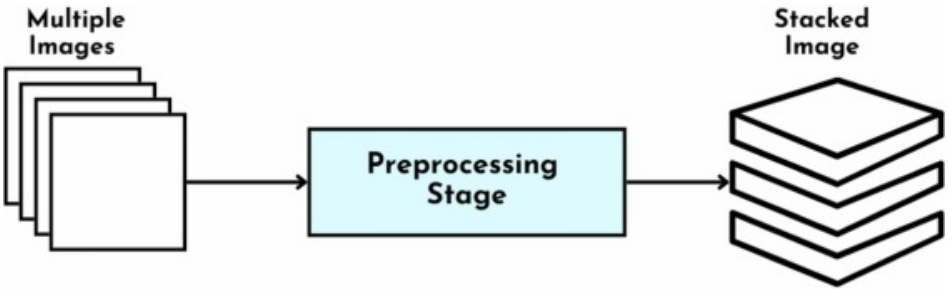


Fig. 2 Stacked image representation

[3] M. Meselhy, et.al.,"Multiple image encryption techniques: Strategies, challenges, and potential future directions,", Alexandria Engineering Journal, vol.125, pp.367-387, 2025.

The AIR helps to reduce the time of encryption and simplify the encryption process, because it encrypts one large image rather than several smaller ones. However, a significant limitation is that the augmented image is larger than the original image, which can make it difficult to store or transmit in bandwidth-limited environments. Moreover, SIR is particularly useful for methods that require multi-dimensional transformations or complex scrambling, such as 3D chaotic maps or hyper-chaotic systems. The stacking of images enables the encryption method to process multiple images simultaneously without losing the unique characteristics of each image. AIR is the general framework for MIE techniques, as shown in Fig.3, Fig.4 for SIR.

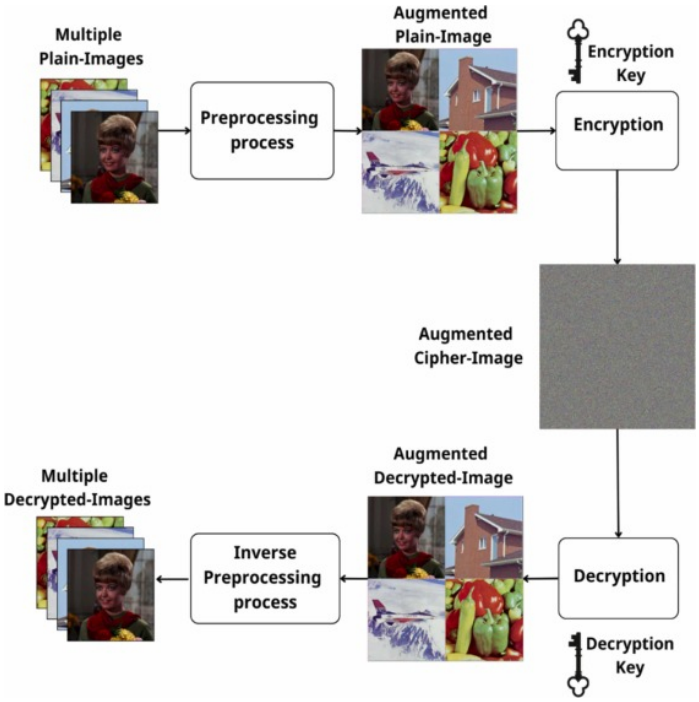


Fig. 3 MIE techniques general framework based on augmented image structure

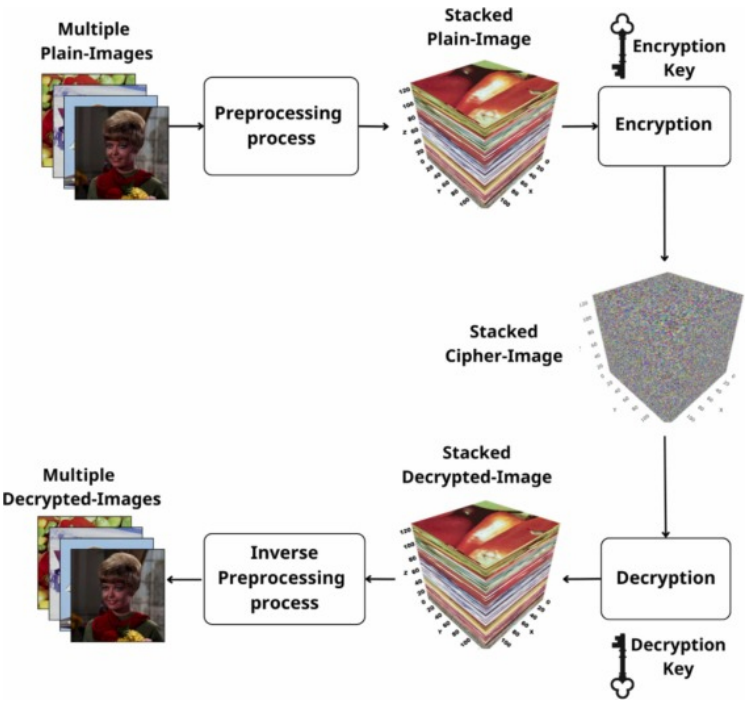


Fig. 4 MIE techniques general framework based on stacked image structure.

2- Literature review

A multi-image encryption algorithm based on bit-plane decomposition, dynamic DNA coding, and image hash is suggested in [4]. The suggested algorithm first creates the initial key for chaotic mapping by combining multiple grey images and using an image hashing algorithm. Second, the bit plane of the combined image is broken down using the random sequence produced by the enhanced three-dimensional chaotic map, and the bit-plane matrix is numerically replaced. The final multiple ciphertext images are produced by decomposing the pixel matrix, and dynamic DNA coding and calculation are carried out on the image using the random sequence produced by the four-dimensional hyperchaotic system. The experimental findings demonstrate that the suggested algorithm can withstand a number of common attacks, including statistical analysis, differential attack, exhaustive attack, cropping, and noise attack, and that it has a large key space, strong key sensitivity, strong security, and robustness.

A bit plane and chaos-based multiple-image encryption algorithm is proposed in [5] to increase the security of image transmission. In order to create k encrypted images, the first step is to decompose k images into 8k bit planes. Next, the pixel positions of the 5th and 8th bit planes of each image are jumbled using the Chen chaotic system and a two-dimensional logistic map. Finally, the scrambled bit planes and all of the 1st–4th bit planes are randomly combined to create k scrambled images. The suggested algorithm's benefits include

[4] Q. Zhang, et.al.,"Multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding", IET Image Processing, vol.15, Issue 4, pp. 885-896, 2020.

a large key space, high encryption efficiency, excellent encryption effect, key sensitivity, and a strong defense against brute-force and statistical attacks, according to experimental results and algorithm analyses.

A DNA-chaos algorithm-based multi-image encryption scheme is proposed in [6] under the computational integral imaging framework. The efficiency of image encryption is greatly increased in this scheme by using a computational integral imaging algorithm to merge multiple images into a single image. In the meantime, the computational integral imaging algorithm can combine images at various depths; as a result, the various depths of several images can also be utilized as keys to strengthen the encryption technique's security. Additionally, to counteract the outline effect brought on by the DNA encryption algorithm, the high randomness of the chaos algorithm is combined. Our experimental verification of the suggested multi-image encryption scheme has been completed. The encoded image's entropy value is 7.6227, while the merge image with two input images has an entropy value of 3.2886. This significantly diminishes the image's relevance. Additionally, the simulation results validate that the suggested encryption work.

The paper in [7] suggests a multiple-image encryption algorithm based on three-dimensional (3D) bit planes and genetic central dogma. The genetic central dogma is simulated and the 3D bit planes are defined in this paper. First, a 3D matrix is created from k original images that have been converted to 8-bit binary; next, the bit plane is rotated and permutations among the bit planes are performed; finally, the jumbled 3D matrix is encoded into DNA codes. Imitating the genetic central dogma and introducing RNA mutations allows for the diffusion to occur; ultimately, the RNA decoding process yields the encrypted images. Analysis of the algorithm and experimental results show that the suggested algorithm performs well and has high security.

A new multiple image encryption method is designed in [8] using the generalized two-dimensional (2D) Arnold map (AM), reality-preserving two-dimensional discrete fractional Hartley transform (RP2DFrHT), and affine Hill cipher (AHC). Our method uses three color images to create three indexed images. After that, RP2DFrHT produces a real domain output image, and AHC carries out a significant amount of confusion and diffusion operations. Finally, the pixel position of the image is shifted by 2D AM. Following the encryption procedure, a single-channel real-valued encrypted image is produced, making it easier to view, store, and send an image over an unprotected network. The suggested method has multiple layers of security in the frequency, time, and coordinate domains. Furthermore, the proper decryption of our method depends on the used parameters, their configurations, and the secret keys. outcomes of simulations, security evaluations, statistical evaluations, and comparisons.

In the Fresnel-transform domain and computational ghost imaging, the paper in [9] suggests a multi-image encryption algorithm based on a modified Gerchberg–Saxton algorithm (MGSA). The first step is to implement "one code, one key" using MGSA; the second is to decrease the amount of ciphertext transmission by using phase function superposition and normalization; and the third is to increase the security of the entire encryption system by using computational ghost imaging. High efficiency, straightforward computation, safety and dependability, and reduced data transmission are all advantages of this method for encrypting multiple images at once. Simulation experiments are used to confirm the

[5] Lei Zhang, et.al.,"Multiple-image encryption algorithm based on bit planes and chaos", Multimedia Tools and Applications, vol.79, Issue 29-30, pp.20753 - 20771, 2020.

[6] L. Xiaowu, et.al., "Multi-Image Encryption Method via Computational Integral Imaging Algorithm", Entropy, vol.24, no.7, 2022.

[7] Xiaoqiang Zhang and Jingxi Tian,"Multiple-image encryption algorithm based on genetic central dogma", Physica Scripta, vol.97, no.5, 2022.

[8] S. Sabir, et.al.,"Multi-layer security based multiple image encryption technique", Computers and Electrical Engineering, vol.106, Issue C, 2023.

method's efficacy and security, and correlation coefficient and structural similarity are used to assess the encryption effect.

An encryption algorithm for multiple images that can encrypt any number, size, or kind of image is proposed in [10]. To address the shortcomings of some current chaotic systems and lessen the complexity of chaotic system design, the paper first suggests a two-dimensional chaotic model that can produce a variety of chaotic system types. The improved performance of the generated chaotic systems is demonstrated by sample entropy analysis, Lyapunov exponent, bifurcation diagrams, and phase diagrams. In order to strengthen defense against plaintext attacks, the paper generates a secret key by fusing several images and then using SHA-512. It is no longer necessary to send the size message and secret key separately because the paper embeds the size message of the original image into the fused image pixels. The study concludes by suggesting a simultaneous permutation and diffusion algorithm to increase efficiency and security. Security analysis and experimental simulations demonstrate the suggested algorithm's encryption capabilities.

In [11], the authors suggest a chaotic model that can solve the issue by producing N-dimensional chaotic systems. After establishing the initial parameters of the seed map within the chaotic range, the authors employ modular operations to expand the parameters' range and boost their complexity. As demonstrated by the simulation results, the generated chaotic system exhibits good chaotic dynamics. The author suggests an encryption algorithm for multiple images that is unrestricted by image size, number, or type based on this chaotic model. An algorithm for permutation diffusion based on overlapping blocks improves the defense against plaintext attacks. A newly defined lookup table operation with improved nonlinearity and randomness is designed by the authors and is based on Latin squares. Different encryption levels can be designed by users to balance encryption effectiveness and efficiency by varying the number of Latin squares and the overlapping block parameters. All of the evaluation indexes reach the expected value, and the experimental results demonstrate that the suggested image encryption algorithm can successfully encrypt multiple images.

Based on the logistic map and the infinite collapse map, the authors present a new two-dimensional (2D) crossed hyperchaotic map in [12]. The system in question can display extensive hyperchaotic behavior and good traversal properties, as shown by the analysis of the phase diagram and Lyapunov exponential spectrum. Furthermore, the need for multi-image encryption schemes has increased due to the growing usage of digital images. Because of this, a multiple image encryption (MIE) scheme is proposed based on the given 2D crossed hyperchaotic map. This scheme uses a cross-plane with simultaneous permutation and diffusion to change the values of its positions and pixels across multiple images. To significantly increase the speed and security of information encryption as well as the effectiveness of key calculation, a pixel blur preprocessing technique is introduced. In the end, security analysis and a few simulation examples show that the proposed encryption scheme can block various types of attacks.

Based on fractal geometry and a new spatiotemporal chaos system, the paper in [13] suggests a novel multi-image encryption algorithm. A new Chebyshev Improved Coupled Sine Map Lattice (CICSML)

---

[9] P. Zhang, et.al.," Multiple-image Encryption and Multiplexing Using a Modified Gerchberg–Saxton Algorithm in Fresnel-transform Domain and Computational Ghost Imaging" , Current Optics,and Photonics, vol.7, no.4, pp.362-377, 2023.

[10] Z. Zhou, et.al., "Novel multiple-image encryption algorithm based on a two-dimensional hyperchaotic modular model", Chaos, Solitons & Fractals, vol.173, 2023.

[11] Z. Zhou, et.al , "Multiple-Image Encryption Scheme Based on an N-Dimensional Chaotic Modular Model and Overlapping Block Permutation–Diffusion Using Newly Defined Operation", Mathematics, vol.11, no.15, 2023.

[12] L. Zhou, et.al.,"Multiple-image encryption scheme based on a new 2D hyperchaotic map with blurred pixels", Physica Scripta, vol.99, no.4, 2024.

system is first created by the algorithm using the Coupled Map Lattice (CML) spatiotemporal chaos system as a basis. The results of dynamic behavior testing show that the CICSML system can execute chaotic iterations in both time and space, producing more chaotic sequences, having a wider parameter space, and exhibiting a wider chaotic region than traditional chaos systems. Second, the algorithm generates index control sequences for the synchronous scrambling diffusion phase using Hilbert curve scan scrambling and fractal matrix. The encryption algorithm's efficiency and security are effectively improved by the Hilbert curve scan scrambling's efficiency and the fractal matrix's initial value sensitivity. Lastly, the algorithm uses the multi-image encryption concept.

In [14], a new image encryption method is introduced that uses a custom S-box produced by the XORshift algorithm, RC5 operations, hyperchaotic systems, Singular Value Decomposition (SVD), and permutation techniques. In order to prevent traffic analysis attacks that could compromise individual encrypted images, this algorithm combines multiple satellite images into a single augmented image before encryption. The augmented image is first divided into RGB color channels, and each channel is then encrypted using a four-step procedure. A chaotic sequence is created from a six-dimensional (6D) hyperchaotic system to start the encryption process. Next, SVD is used to manipulate and create a new key from this original key sequence. To add an extra layer of security, the original image is XORed using the altered key sequence. Following that, the image is separated into blocks, and each block is subjected to RC5 operations. The image is then subjected to an S-box, which is made from a random sequence produced by the XORshift algorithm, in order to further mask the pixel values. Numerical tests verify the algorithm's robustness and show that it is effective against brute-force, statistical, and differential attacks. This makes it very difficult for third parties, like cloud service providers, to find any relational patterns between the encrypted satellite images. This encryption technique not only improves the security of satellite imagery against unwanted access but also guarantees the integrity and confidentiality of the images, which are essential for applications ranging from environmental monitoring to national security in a world that is becoming more and more data-driven. Specific numerical values that showed an enhanced security level include a key space of 2^7016, entropy exceeding 7.999, and a cross-correlation of ≈0.

An innovative three-layer multiple-image encryption (MIE) method based on three 2D-chaotic maps is presented in [15]. The RGB channels are separated into each multiple-color image in the first layer. Each channel's images are randomly arranged through a randomization process before being combined to create a single image (batch), which serves as the input for the layer that follows. Using Baker, Henon, and 2-D Logistic chaotic maps, the second layer creates chaotic sequences for independently scrambling pixels in each channel, producing a scrambled image. By independently altering the pixel values in each channel using distinct chaotic sequences produced by the three maps and the XORing operation, the diffusion process is applied in the last layer. Tests such as horizontal, vertical, and diagonal correlation as well as key sensitivity, key space analysis, complexity analysis, and entropy assessment are used to validate the effectiveness of the suggested scheme.

---

[13] L. Huang and H. Gao, "Multi-Image Encryption Algorithm Based on Novel Spatiotemporal Chaotic System and Fractal Geometry," IEEE Transactions on Circuits and Systems, vol. 71, no. 8, pp. 3726-3739, 2024.

[14] M. Youssef et al., "Enhancing Satellite Image Security Through Multiple Image Encryption via Hyperchaos, SVD, RC5, and Dynamic S-Box Generation," IEEE Access, vol.12, pp.123921-123945, 2024

[15] Hosny, K.M., Elnabawy, Y.M., Salama, R.A. et al., " Multiple image encryption algorithm using channel randomization and multiple chaotic maps", Scientific Reports, vol.14, 2024.

In order to improve digital image security and speed up transmission, Authors proposed a four-tier multiple image encryption (MIE) technique in [16]. The authors first created an augmented image by attaching the plain images. The second step involves randomly shifting each plain image's location to create the randomized augmented image. Third, the authors used the zigzag pattern, rotation, and random permutation between blocks to jumble the randomized augmented image. The authors then use an Altered Sine-logistic-based Tent map (ASLT) to diffuse the jumbled augmented image. To simplify and make the suggested method easy to understand, the authors create a flowchart, write pseudo-code, and provide an example. The Four-Tier technique was evaluated through a number of experiments, and the findings demonstrate how secure and effective it is against a variety of attacks.

In[17], authors propose a way to encode multiple images at once using chaotic one-dimensional (1D) maps. First, each grayscale image is consolidated into one large image. Each block is permutated parallel to each other through transpose columnar transposition and bit-XOR diffusion procedures. The parallel permutation and diffusion functions are used to speed up and improve the method. Unlike other multi-image encryption methods, the proposed algorithm always uses a single 1D chaotic map, making the algorithm both software and hardware efficient and simple. This technique is consistent with general requirements for simplicity and high efficiency. The proposed method is straightforward, highly effective, and effectively improves the security of cipher images, and security analysis and simulation results show that the proposed method is effective, straightforward, and highly effective.

The article in [18] suggests a new multiple image encryption (MIE) algorithm that combines a chaos-based Hill cipher, counter mode RC5, hyperchaotic systems, Singular Value Decomposition (SVD), and a customized S-box produced by a modified Blum Blum Shub (BBS) algorithm. To improve security against traffic analysis, the suggested MIE algorithm first combines several satellite images into an augmented image. The colored image is divided into RGB channels for encryption, and each channel goes through four stages: substitution with a custom S-box created by a modified BBS, RC5 encryption in counter mode with XOR operations, additive confusion using a memristor hyperchaotic key transformed by SVD, and Hill cipher encryption using a 6D hyperchaotic key and invertible matrices mod 256. The suggested algorithm's improved randomness, superior encryption efficiency, and robustness against brute-force, differential, and cryptanalytic attacks are all demonstrated by experimental results. These results demonstrate how the MIE algorithm can protect satellite imagery in real-time applications while maintaining confidentiality and resilience to contemporary security risks.

A multi-image encryption algorithm is presented in [19]. A chaotic system and wavelet transform-based key generation algorithm is presented in the first step of the suggested algorithm. The encryption algorithm is then developed by introducing chaotic system-based rearrange and shift functions. The hybrid chaotic system, which is produced by fractional derivatives and the Cat map, is one of the most crucial tools in the suggested algorithm. The effectiveness of the suggested hybrid system is shown by a variety of tests that were used to examine its behavior. Several statistical and security tests, such as data loss and noise attack simulations, correlation coefficient analysis, and histogram analysis, have been conducted on the suggested

[16] Hosny, K., Kamal, S. A new four-tier technique for efficient multiple images encryption. Multimedia Tools and Applications, 2024.

[17] K. Abhimanyu, et.al., "Chaotic multiple-image encryption scheme: a simple and highly efficient solution for diverse applications", Journal of Electronic Imaging, vol. 33, Issue 4, 2024.

[18] W. Alexan, et.al., "A new multiple image encryption algorithm using hyperchaotic systems, SVD, and modified RC5",Scientific Reports vol.15, Article number: 9775, 2025.

algorithm in the final stage of the suggested approach. The outcomes demonstrate how well the suggested algorithm works for secure transmission.

3. Conclusion

The current state of research on multiple image encryption (MIE) algorithms is thoroughly reviewed in this paper. Although MIE has advanced significantly, there are still a number of important issues that need to be addressed, according to one of the literature review's main conclusions. Concerns about computational efficiency, ideal parameter selection, and security flaws are urgent. Computational speed is especially important for real-world applications because many current approaches find it difficult to strike a balance between security, robustness, and real-time processing. Moreover, the field of multiple-image encryption is still developing and needs more innovation and improvement. The need for more research in this area is highlighted by the rising demand for safe and effective encryption methods in cloud storage, secure communications, and multimedia applications. To solve these enduring problems, future research should concentrate on creating encryption frameworks that are more secure, effective, and flexible.

[19] G. Ghasemi, et.al.,"Three-Dimensional and Multiple Image Encryption Algorithm Using a Fractional-Order Chaotic System", Computation, vol.13, no.5, 2025.

Iran's Nuclear Doctrine Shift and Its Ballistic Missile Arsenal as a Delivery Platform

Mehran Atashjameh

Introduction

Recent statements from Iran's parliament suggest a possible shift in the nation's nuclear and military strategy in response to what it perceives as threats from Israel and the United States.[1] In recent months, Iran's officials reinforced their stances by affirming Iran's technical ability to produce nuclear weapons and indicating a readiness to reconsider the nation's nuclear doctrine if Iran's existence is at risk. This matter highlighted that while Iran's nuclear ambitions have so far been restricted by a 2003 fatwa from Khamenei banning nuclear arms, this position could change if security threats escalate. Furthermore, Kharrazi suggested Iran may enhance the range of its Ballistic Missiles (BMs), adding another dimension to the country's defensive and offensive capabilities. Adding to these statements, General Mohammad Naeini of the Islamic Revolutionary Guard Corps (IRGC) warned that any enemy aggression would be met with a powerful and strategic response. He explicitly cautioned Israel, emphasizing that any hostile act would be met with a retaliation "beyond the enemy's comprehension." [2] [3] [4] The key themes from these statements focus on " Iran's ability and possible shift towards nuclear weapon production" and "enhancement in BM's arsenal as a Delivery System (DS)". The rhetoric from Iranian officials highlights a readiness to escalate their defense strategy if they perceive an existential threat, positioning these developments as deterrents against future hostilities from the U.S. and Israel. However, while successfully designing a nuclear weapon is essential, effective deterrence hinges on the availability of a "reliable DS" to ensure its readiness and impact. This article proceeds as follows: the first section outlines the concept of delivery systems; the second examines the importance of reliability in such systems; the third analyzes Iran's ballistic missiles as the most plausible delivery option; the fourth briefly considers Iran's air force as a potential alternative; the fifth evaluates recent operations to assess the operational reliability of Iran's ballistic missiles; and the final section draws conclusions based on the available evidence

Keywords: Ballistic Missile, Iran, Delivery System, Reliability

[1] Iran International, "Iranian suggested urge review of defense doctrine, call for nuclear weapons", Iran International, 2025. <https://www.iranintl.com/en/202509229643>

[2] Aurora Almendral, Amin Khodadadi and Andrew Jone, ' Iran says it has the capacity to make nuclear weapons; supreme leader threatens U.S. and Israel', NBC News, 2024. <https://www.nbcnews.com/news/world/iran-nuclear-doctrine-change-israel-hezbollah-rcna178406>

[3] Reuters, ' Iran adviser hints at expansion of missile range, nuclear doctrine review after Israel strikes', Reuters, 2024. < https://www.reuters.com/world/middle-east/iran-adviser-hints-expansion-missile-range-nuclear-doctrine-review-after-israel-2024-11-01/>

[4] Patrick Sykes, "Iran's Parliament to Debate Changing Peaceful Nuclear Doctrine", Bloomberg, 2025. <https://www.bloomberg.com/news/articles/2025-09-26/iran-s-parliament-to-debate-changing-peaceful-nuclear-doctrine>

Delivery Systems

DSs are how nuclear weapons are deployed and delivered to their targets, playing a crucial role in a nation's nuclear strategy. These systems can include land-based Intercontinental Ballistic Missiles (ICBMs), Submarine-Launched Ballistic Missiles (SLBMs), and strategic bombers, each offering distinct advantages and capabilities. The effectiveness of a nuclear force is often assessed by the survivability and "reliability" of its DSs, as well as its ability to penetrate enemy defenses. For example, the United States employs a nuclear triad, consisting of land-based ICBMs, SLBMs, and strategic bombers. This triad ensures a diversified and resilient nuclear deterrent, allowing the U.S. to respond effectively to a nuclear attack and maintain a second-strike capability, thereby deterring potential adversaries through the assurance of a credible retaliation.[5] The "reliability" of DSs for nuclear forces depends on a shared understanding among adversaries that each side has a "reliable" and capable means to respond to an attack in kind.[6]

Reliability and Delivery Systems

It is critically important that DSs be reliable in delivering nuclear weapons, as the credibility of a state's nuclear deterrent depends not only on the existence of these weapons but also on the assurance that they can be effectively deployed when required. If a DSs fails to function as intended, it could undermine deterrence, increase strategic uncertainty, and heighten the risk of miscalculation during crises. Hence, nuclear-armed states conduct regular cycles of tests and evaluations of their missiles, submarines, and bomber aircraft. These tests serve multiple purposes: they verify the technical performance of the DSs under realistic conditions.[7] Through these rigorous testing programs, states aim to minimize the risk of failure and sustain a credible nuclear posture capable of responding to urgent threats.

Iran's Ballistic Missile Arsenal as Delivery Option

Iran's pursuit of missile technology began before the 1979 Islamic Revolution, spurred by its role as a Western ally against Soviet influence and by the Nixon Doctrine, which encouraged U.S. allies to strengthen their own defenses. During the Shah's reign, Iran aimed to build regional power, significantly investing in military advancements. Initial efforts included the Arash rocket system, based on the Russian BM-11, and collaboration with Israel on "Project Flower" to develop surface-to-surface missiles.[8] The 1979 Islamic Revolution brought a sharp political shift and led to U.S. sanctions that restricted Iran's access to arms.[9] In 1980, Iraq's invasion of Iran and the ensuing Iran-Iraq War catalyzed Tehran's focus on BMs after Iraqi SCUD missile attacks on Iranian cities which was known as "War of Cities".[10] Iran initially sourced SCUD-B missiles from Libya[11] and later secured additional SCUDs and technical assistance from North Korea,[12] helping build Iran's missile arsenal. After the Iran-Iraq War, Iran continued to advance its BM program, relying on partnerships with universities, domestic industries, and international allies like North Korea, China, and Russia. These efforts enabled the production of the Shahab missiles, based on SCUD models, with ranges up to 580 kilometers.[13]

---

5 Nuclear Matters Handbook, 'Nuclear Delivery Systems', Acquisition and Sustainment Office of The Under Secretary of Defense, 2020, 2-3. <https://www.acq.osd.mil/ncbdp/nm//NMHB 2020rev/docs/NMHB2020rev_Ch3.pdf>

6 Indo-Pacific Defense forum, 'Improving Strategic Deterrence', Indo-Pacific Defense forum, 2023. <Improving Strategic Deterrence – Indo-Pacific Defense Forum>

7 National Academies Press, "The Comprehensive Nuclear Test Ban Treaty: Technical Issues for The United States - Safety, Security, And Reliability of The U.S. Nuclear Weapons Stockpile", National Academies Press, 2012. <https://nap.nationalacademies.org/read/12849/chapter/4>

Over time, Iran has developed BMs with ranges reaching 2,000 kilometers, now forming the largest BM arsenal in the Middle East.[14] Mobile launch platforms and underground facilities have strengthened Iran's missile capabilities to protect these assets. By the 1990s, Iran had acquired mobile Transporter Erector Launcher (TEL) platforms from North Korea and developed its own TELs, emphasizing mobility to avoid detection and improve deterrence.[15] Additionally, Iran invested in hardened underground bunkers, creating "Missile Cities" to safeguard its strategic assets from potential strikes. In Parallel, Iran's space program, with roots dating back to the 1950s, shares technology with its BM program, allowing for further BM advancement under the guise of space exploration. Post-war, Iran has used BMs not only as a deterrent but in direct military actions, including strikes on opposition groups, U.S. forces in Iraq, and recently on Israel demonstrating their role as operational weapons rather than merely defensive assets.

In summary, Iran's BM program, developed amid sanctions and regional conflicts, has become integral to its military strategy, supported by both international cooperation and domestic efforts to localize missile technology. Iran's extensive BM arsenal now serves as a primary element of its defense and deterrence doctrine, capable of both strategic and offensive operations across the region.[16]

Air Force Fleet as an Alternative?

During the pre-1979 era, Iran's air force reached a significant level of advancement due to the Shah's substantial investments and close ties with the United States, which was its primary supplier of advanced military equipment. However, the 1979 Islamic Revolution marked a turning point.[17] The severance of U.S.-Iran relations, coupled with the imposition of sanctions, left Iran unable to procure spare parts or modernize its fleet. The devastating eight-year Iran-Iraq War further eroded the air force's capabilities as sustained combat operations, attrition, and logistical difficulties took a heavy toll.[18]

Hence, In the post-war period, Iran attempted to rebuild its air force by acquiring new aircraft and some that evacuated from Iraq during the Persian Gulf War.[19] Despite these additions, the combined effects of Western sanctions and Iran's inability to procure or develop advanced fighter jets have prevented the air force from regaining its former power. The aging fleet has been plagued by frequent crashes, underscoring its declining reliability and safety.[20] Consequently, when considering Iran's air force as a potential delivery platform for nuclear weapons, it is crucial to account for the air force and air defense capabilities of U.S. and its allies in the region specifically Israel, Iran's determined rival. Israel, in contrast, has consistently upgraded its air force and acquired advanced systems over the decades, maintaining a significant technological edge.[21]

---

8 The Nuclear Threat Initiative, "Iran Missile Overview", The Nuclear Threat Initiative, 2017. <https://www.nti.org/analysis/articles/iran-missile/>

9 Sam Sasan Shoamanesh, " History Brief: Timeline of Us■Iran Relations Until The Obama Administration", Massachusetts Institute of Technology, 2009, 3-4. <https://web.mit.edu/mitir/2009/online/us-iran-2.pdf>

10 Douglas A. Kupersmith, "The Failure of Third World Air Power, Iraq and The War With Iran", Air University Press, 1993, 33-37. <https://apps.dtic.mil/sti/pdfs/ADA425672.pdf>

11 Directorate of Intelligence, "The Iranian Missile Threat", Central Intelligence Agency (CIA), 1985, 3. <https://www.cia.gov/readingroom/docs/CIA-RDP85T01058R000406030001-3.pdf>

12 Iran Watch, "A History of Iran's Ballistic Missile Program", Wisconsin Project on Nuclear Arms Control, 2012. <https://www.wisconsinproject.org/a-history-of-irans-ballistic-missile-program/>

20 Paul Iddon, " Iran's Vintage Fighter Jets Keep Falling Out Of The Sky", Forbes, 2022. <https://www.forbes.com/sites/pauliddon/2022/05/29/irans-vintage-fighter-jets-keep-falling-out-of-the-sky/>

Operational Assessment

Toward assessing Iran's ballistic arsenal as potential option for deploying nuclear weapons, considering the operational assessment is crucial. In recent years, Iran has conducted several BM strikes, and these actions underscore the growing importance of BMs in Tehran's defense posture. These strikes including those on ISIS bases in Syria[22], the Ain Al-Asad base in Iraq[23], the operations True Promise I[24] and True Promise II[25], June conflict with Israel[26], and ongoing tension between Iran, the united States, and Israel[27] provide valuable data for assessing Iran's BMs as potential DSs for a probable future nuclear force. Iran's BMs have improved in recent years, exemplified by the unveiling of advanced systems such as the Fattah family class[28], which are capable of performing maneuvers in the terminal phase to penetrate air defense interceptors. These advancements have enhanced Iran's operational capabilities, particularly in penetrating Israel's advanced multi-layered air defense network and achieving greater accuracy.[29]

However, recent strikes, specifically those which conducted in 2024 and 2025, strikes also demonstrate that Iran BMs have experienced in-flight failure rates that affect their overall reliability.[30] [31] These failures can arise from various causes, such as technical issues. Additionally, non-technical factors have also been highlighted for example, Mohammad Bagher Ghalibaf, Speaker of the Iran Parliament, stated in an interview about the True Promise I operation that defective parts introduced by external actors had affected Iran's BM performance. He compared this to Israel's reported interference with Hezbollah's walkie-talkies and pagers.[32] This claim underscores that the reliability of Iran's BMs is influenced by multiple factors, including technical aspects, supply chain vulnerabilities, and operation-security[33] measures, as a measure of passive defense. However, in the ongoing 2026 conflict, Iran's ballistic missile strikes against Arab states in the Persian Gulf theatre suggest that its SRBMs demonstrate higher reliability, fewer inflight failures, and greater precision partly due to targeting air and missile defense assets[34] compared with its longer-range platforms[35].

---

13 Richard Speier, Rober Gallucci, Robbie Sabel, Victor Mizin, "Iran-Russia Missile Cooperation", Carnegie Endowment for International Peace, 2-4. <https://carnegieendowment.org/files/Repairing_12.pdf>

14 Erik A. Olson, "Iran's Path Dependent Military Doctrine", Strategic Studies Quarterly, 2016, 69-70. <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/Olson.pdf>

15 Farzin Nadimi, "Iran's New Ballistic Missile May Have North Korean ICBM Links", The Washington Institute For Near East Policy, 2017. <https://www.washingtoninstitute.org/policy-analysis/irans-new-ballistic-missile-may-have-north-korean-icbm-links>

16 Mehran Atashjameh, "Passive Defense measures in Saving Iran's ballistic Missile arsenal", Marine Corps University-Middle East studies (MES Insight), 2024, 2-4. <https://www.usmcu.edu/Portals/218/MES%20Insights_Atashjameh_15_4.pdf>

Conclusion

Iran's BM arsenal, shaped by decades of investment and the shortcomings in modernizing its air force, has become a central element of Tehran's defense doctrine. In light of official Iranian statements regarding a potential shift in nuclear doctrine and the characterization of the BM arsenal as a delivery platform, reliability has become a central concern. in this context, should Iran pursue nuclear armament of its missiles, available evidence suggests that while the overall BM arsenal carries reliability risks, SRBMs appear to have a higher likelihood of dependable performance compared with medium-range ones. This arsenal includes a variety of missile classes, both solid- and liquid-fueled, across different ranges, capable of delivering payloads of varying yield, and advancing not only theoretically but also operationally. Nonetheless, recognizing Iran's BMs as fully reliable delivery systems remains uncertain, particularly for high-stakes non-conventional strikes, where missile failure could risk the loss of strategic payloads. Therefore, Tehran's decision-makers must acknowledge that establishing credible nuclear deterrence through their BM arsenal involves not only acquiring nuclear weapons but also developing highly reliable delivery systems with minimal probability of failure

[18] Michael Eisenstadt, "Iran after Sanctions: Military Procurement and Force-Structure Decisions", International Institutre of Strategic Studies (IISS), 2017, 2. <https://www.iiss.org/globalassets/media-library---content--migration/images/comment/analysis/2017/december/3-eisenstadt2125.pdf>

[19] Michael Brill, "Remembering Desert Storm and the Gulf War(s) Odyssey of Iraq's Air Force", Wilson Center, 2021. <https://www.wilsoncenter.org/blog-post/remembering-desert-storm-and-gulf-wars-odyssey-iraqs-air-force-part-1>

[27] Council on Foreign Relation (CFR), "Iran's War With Israel and the United States", CFR, 2026. <https://www.cfr.org/global-conflict-tracker/conflict/confrontation-between-united-states-and-iran>

[28] Fabian Hinz, "Removing the hype from Iran's 'hypersonic' conqueror", Institute for Strategic Studies (IISS), 2023. < https://www.iiss.org/online-analysis/military-balance/2023/07/removing-the-hype-from-irans-hypersonic-conqueror/>

Cybersecurity Vulnerabilities in U.S. Communication Infrastructure and Strategies for Risk Mitigation

Josh Reid

ABSTRACT

There are many vulnerabilities to the United States Critical Communications Infrastructure. This infrastructure is crucial to national security and the wellbeing of our nation. This paper examines these vulnerabilities through methodology and case studies. This paper highlights the three primary cyber threats: Ransomware, Malware, and Distributed Denial of Service attacks (DDoS). These attacks present the greatest risk to critical communication infrastructure.

This paper also explores cases studies from the AT&T data breach and Baltic Undersea Cable Sabotage. The AT&T data breach was a ransomware attack that illustrates the dangers to telecom networks through theft, and extortion. The Baltic undersea cable sabotage underscores physical threats to critical communication infrastructure. These cases identify the need for enhanced policies, and a shift in perspective towards long term cyber strategy.

Additionally, this paper analyzes key actors that pose a threat to critical communication infrastructure. China, Russia, and Iran are all state actors who have strong political motivations. Non-State Actors also are significant threats for various reasons. Finally, internal bad actors either by malicious or negligent means are risks.

A standardized threat-assessment framework is needed to classify and define cyber-attacks. Type A attacks are physical attacks on hardware, Type B attacks are software exploitations, Type C attacks are hybrid attacks that can involve political and other areas in conjunction with an attack.

Further federal agency oversight is needed to prevent and respond to cyber threats. Mandating regular reporting, and robust public-private partnerships will be best practice for cyber threats. Additionally, alternative networks are needed in the event of widespread failure. Satellite Mesh Networks should be used in the event of an emergency to establish reliable redundant communications.

Introduction

Innovations in technology improve the efficiency of society. Critical infrastructure now relies on internet connectivity and technology to function. These innovations bring wonderful benefits that enrich lives and maximize efficiency. However, cyber threats also exploit innovations for political and economic gain in our critical infrastructure. Knowbe4, a global security awareness platform, released a report on cyberattacks on critical infrastructure in 2024. "Critical infrastructure worldwide sustained over 420 million attacks – equivalent to 13 attacks per second – marking a 30% increase from 2022."[1] Cyber-attacks will certainly increase in the future. The last three years have shown similar increases like the 30% increase in 2022. It is imperative to defend critical infrastructure from such attacks. These attacks cripple states and deprive people of access to basic needs and resources.

One area of critical infrastructure that has vulnerabilities, is Communication critical infrastructure. Exploitation of this infrastructure could lead to communication networks being totally disabled. This would disrupt every area of our lives. Communication critical infrastructure, specifically cellular and internet infrastructure, are cornerstones of national stability. Finance, healthcare, defense, and other critical infrastructure areas depend on communication infrastructure to function.

In addition to the threats themselves, there are many challenges in developing and executing strategies to protect and defend communication infrastructure. Cyber threats evolve so quickly that traditional defense strategies can't adapt fast enough. "In the IT sector, there is a constant arms race of technological development leading the way with security evolving to address new vulnerabilities. Whenever a new technology is implemented, there is a potential for new "zero-day" exploits, or attacks that are undiscovered and unknown by anyone except for the attacker."[2] It is impossible to account for every new technology and prepare a specific strategy for each. That is why creating a framework that is adaptable to new threats is essential. Through analyzing previous incidents and applying lessons learned we can develop and implement new frameworks and solutions.

This paper will answer the question "What vulnerabilities exist in the U.S. communication infrastructure from cyber-attacks, and what measures can be implemented to mitigate risk? Understanding and closing vulnerabilities is only the first step to protecting crucial communication infrastructure. In the U.S we are majorly underprepared to deal with large scale cyberattacks. If a cyber-attack happened today, it could cause damage to the critical communication infrastructure that would have major consequences. Cyberthreats change so quickly in today's world that nations must develop solutions that adapt to evolving attacks. This can be done by developing a threat assessment framework, viewing cyberthreats in the long-term, and incentivizing public-private cooperation

[1] KnowBe4, "KnowBe4 Report Reveals Critical Infrastructure under Siege with Cyber Attacks Increasing 30 Percent in One Year," 2024, https://www.knowbe4.com/press/knowbe4-report-reveals-critical-infrastructure-under-siege-with-cyber-attacks-increasing-30-percent-in-one-year

[2] Engel, Cyber Infrastructure: Challenges and Strategies (College Station: Bush School of Government & Public Service, Texas A&M University, 2011), https://bush.tamu.edu/wp-content/uploads/2020/02/Engel_Spring2011.pdf.

Identifying Vulnerabilities through Case Studies

There are three main types of attacks on critical infrastructure Ransomware, Distributed Denial-of-Service (DDoS), and Malware. These three attacks are most common and encompass most other subcategories of attack. Each exploits a different vulnerability and is used for different purposes. Having a basic understanding of each attack is key to building better approaches to defend our communication infrastructure.

Ransomware attacks steal and or encrypt data and demand a ransom payment for its release. This can be thought of like the taking of a hostage. A report by Sophos Security Firm saw 59% of organizations hit last year by some form of ransomware.[3]These attacks are generally motivated by economic gain in order to release data. These attacks are by far the most common. A bad actor will exploit vulnerabilities to obtain access to a system. They then deploy bad software that locks or disrupts service and demand payment to release. A recent example of this was the Colonial Pipeline in 2021.

DDoS attacks overwhelm a targets network and devices with massive amounts of traffic. This causes services and devices to be inoperable. This attack is severely concerning as its sole purpose is to destroy and cripple infrastructure. DDoS can be used with great success on communication infrastructure. A bad actor could use this to flood telecom networks with traffic exceeding the capacity of a tower. This will overload the system and cause an outage.

Malware attacks infiltrate systems and execute malicious code. These can have effects ranging from spyware to gather intelligence and further access, to disruptive pieces of code that steal and damage data. The Office of the Director of National Intelligence (ODNI) states on their website that “The persistent and evolving nature of threats to critical systems.” Malware infections often serve as entry points for larger-scale attacks, making robust cybersecurity policies essential.”[4] Malware attacks are commonly used by state actors and state actors associated groups to collect intelligence and steal data. A bad actor could use this by obtaining access to a telecom company and deploying malware. When activated this malware could steal, erase, or duplicate data to create a massive disruption.

Less complicated yet no less important, physical attacks on communication infrastructure pose a significant threat. These attacks can range from damaging cell towers, cutting fiber optic cables, or sabotaging key network hubs. Even a single well-placed attack can disrupt internet access, phone service, and emergency communications. When properly executed, physical attacks can deal catastrophic blows, crippling entire regions, hindering response efforts, and causing widespread economic and social instability.

---

[3] Sophos, The State of Ransomware 2024 (2024), https://www.sophos.com/en-us/content/state-of-ransomware

[4] Office of the Director of National Intelligence, Recent Cyber Attacks on U.S. Infrastructure Underscore Vulnerability of Critical U.S. Systems (June 2024), https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

AT&T Data Breach

An incident in April of 2024 exemplifies just how vulnerable our communication infrastructure is. This attack exploited a third-party cloud platform to steal AT&T customers call logs, texts, social security numbers, and other sensitive pieces of data. The hackers that stole this data remain unknown to this day and if they were part of a state-sponsored attack. One severe consequence of these attacks is theft of sensitive data. This could include sensitive or confidential data vital to national security. The theft of this data could lead to adversaries obtaining critical information we do not want them to know. "Imagine if the records show communication between high-value individuals from organizations that may be currently in confidential business talks about joint ventures, mergers, etc. Perhaps important public officials are in these call records. So, the potential for additional risks to these individuals and organizations cannot be ignored."[5] Naturally because of this risk the FBI was involved in investigating this attack. While these breaches did not disrupt service of any kind, they represent very risk of attack, and the next breach may deal significantly more damage.

This attack was a form of ransomware. The hackers stole sensitive information and demanded payment for the deletion of it. Although it differs slightly from a traditional ransomware attack, this hostage situation falls under a ransomware classification. AT&T reportedly paid around $370,000 to these hackers after the attack.[6] Although this is a relatively small amount for compensation, it signals to cybercriminals that telecom networks will pay criminals.

The two main threats and takeaways from this attack are clear. First, networks can and will be breached. Advanced security measures are important, but they will not stop every attack. Sophisticated cyber threats find innovative solutions to breach networks. Second, the risk of long-term sabotage is a critical concern. Only looking at this specific incident may lead one to believe that it was an isolated attack. However, the possibility remains of coordinated attacks over time to weaken infrastructure and cause systemic failures. ODNI warns that "State-sponsored cyber actors continue to target critical infrastructure as part of broader geopolitical strategies."[7] It is vital to consider these breaches and attacks as possibly part of a long-term goal.

Baltic Sea Cable Sabotage

While the following case study occurred in Europe, it perfectly illustrates potential threats the U.S could face and should prepare for. In late 2024, an undersea power cable connecting Finland and Estonia (Estlink-2) was severed by a passing ship. This caused disruption in data transmission and raises serious concerns of sabotage. It is suspected that a Russian backed proxy group carried out the attack on the undersea cables. Attacks such as these can be detrimental to states heavily dependent on the internet as almost all global internet traffic goes through these cables. This sabotage raises concerns of critical communication sabotage by foreign adversaries. As the U.S is very dependent on internet connectivity via undersea cables, this type of sabotage would be very effective at disrupting our state.

---

[5] S. Benton, "What the Latest AT&T Breach Tells Us," Security Info Watch, 2024, https://www.securityinfowatch.com/cybersecurity/article/55131369/what-the-latest-att-breach-tells-us

[6] E. Kovacs, "AT&T Breach Linked to American Hacker, Telecom Giant Paid $370K Ransom," SecurityWeek, 2024, https://www.securityweek.com/att-breach-linked-to-american-hacker-telecom-giant-paid-370k-ransom-reports/

[7] Office of the Director of National Intelligence, Recent Cyber Attacks on U.S. Infrastructure Underscore Vulnerability of Critical U.S. Systems (June 2024), https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

This attack is an example of physical attacks on cyber hardware. These physical attacks on undersea cables are very damaging and difficult to control. In remote ocean seabed's where these cables lie, there is a great difficulty to monitor and protect them. Not only are they difficult to reach, but they can be in international waters or places where states have limited jurisdiction.

In the U.S we rely on undersea cables to connect us to all parts of the world. These cables are the underappreciated backbone of the U.S economy and identity. It is vital to protect these cables. The case study in the Baltics is also a warning to the U.S adversarial states and or non-state actor group would likely target these cables to sabotage the U.S.

Actors Posing a Threat

Understanding who is carrying out attacks, as well as motivations for attacks can help the U.S prioritize defensive strategies for our communication infrastructure. A variety of adversarial states and non-state actors pose a threat to the U.S there are even internal actors that can also pose a great threat. Identifying these actors is key to finding innovative solutions to protect critical infrastructure.

China

China is a major threat to the U.S in terms of cybersecurity. China actively sponsors attempts to steal user data, sabotage critical infrastructure, and influence U.S citizens. A joint advisory from the Cybersecurity and Infrastructure Security Agency (CISA), advised the public that Chinese sponsored hacking groups are trying to pre-position themselves for cyber-attacks on U.S critical infrastructure in the event of a conflict[8]. China typically uses proxy groups or third-party actors to hide involvement in attacks. With their rapid development into AI and other emerging technologies. China poses a serious threat to U.S Critical Infrastructure.

China’s motivations mostly stem from political and economic gain. As rival superpowers, China has a lot to gain from competing with us economically. By gathering intelligence, and sabotaging key sectors, China hopes to earn a competitive advantage. China also seeks political advantage. One report suggests that China is targeting prominent political figures telecommunications. Leaders like President Donald Trump, and staffers from Kamala Harris’s campaign were targeted as an attempt to influence the 2024 election.[9]

Russia

Russia is a very adversarial state in terms of cyber warfare. Russia has launched many attacks and attempted sabotage over the last 10 years. The GRU (Main Intelligence Directorate) which is the Russian military intelligence has been linked to many forms of cyber-attacks. The Baltic Sea Cable sabotage is one possible example of this.

The motivations of the Russian government are much different than that of China. Russia seeks to undermine the U.S and its strong alliances. The Center for Strategic and Internation Studies in Washington

[8] Cybersecurity and Infrastructure Security Agency, APT Actors Exploit Ivanti Vulnerabilities in Federal Agencies and Critical Infrastructure Organizations (AA24-241A) (2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a

[9] M. Green and J. Moolenaar, “China Attacked U.S. with Hackers. We Need to Hit Back Hard,” U.S. House of Representatives, 2024, https://homeland.house.gov/2024/12/16/china-attacked-us-with-hackers-we-need-to-hit-back-hard-chairmen-green-moolenaar-pen-new-counter-ccp-op-ed/

D.C lists these objectives “Influencing public opinion, coercing governments to curb military and other assistance to Ukraine, create fissures between NATO and allies, and undermine democratic norms and values in the west”.[10] While China may be a more prominent adversary, Russia may be the more dangerous. Its motivations only exist to sabotage and undermine the U.S. In reference to critical infrastructure, Russia would prefer means of sabotage that destroy infrastructure and cause chaos. Both leaders of the CIA and MI6 described Russian intelligence activity as a ‘reckless campaign of sabotage across Europe” stating that Russia’s use of technology to “spread lies and disinformation” was designed to sow division.[11]

Iran

Iran has developed growing cyber capabilities. State sponsored groups are largely responsible for attacks. Iranian hacking incentives primarily target government critical infrastructure and typically deploy tactics such as ransomware and other malware that steals sensitive data.[12]

Iran’s motivations are largely retaliatory. They typically launch attacks in response to heightened geopolitical tensions. Iran will launch attacks after events like the assassination of Irania military leaders, or imposition of sanctions. These hackers use their attacks to strike back against the U.S. ODNI reports that Iran also uses attacks as a tool of psychological warfare to create fear and uncertainty against the U.S and its people.[13]

Internal Threats

In addition to foreign threats. There are also internal threats that pose a risk to vulnerabilities in communication critical infrastructure. These insiders can either operate on behalf of foreign governments or alone. Insiders pose a great risk due to their direct proximity to the systems and trust of network administrators.

There are two main types of insider threats. Malicious insiders are those who seek to attack infrastructure because of ideological reasons, as a form of domestic terrorism, or for economic gain. Then there are negligent insiders. These are individuals who due to their negligence, such as poor maintenance of systems or insufficient cybersecurity, cause issues that open vulnerabilities in our infrastructure.

One example of an insider threat occurred in 2021. A recently fired employee at a regional credit union became extremely disgruntled after her termination. Due to this, she decided to extract revenge on the company. Before the internal IT team could revoke her access, she accessed and deleted over 21 GB of various critical files and programs. Some of these files contained anti-malware and anti-ransomware protocols.[14] This instance shows how indirect actions can lead to cyber-risk. In this case without anti-malware and anti-ransomware protections, this credit union could be vulnerable to cyber-attacks. Similar things can occur in critical communication organizations.

---

[10] S. Jones, Russia’s Shadow War against the West (Center for Strategic and International Studies, 2025), https://www.csis.org/analysis/russias-shadow-war-against-west

[11] S. Jones, Russia’s Shadow War against the West (Center for Strategic and International Studies, 2025), https://www.csis.org/analysis/russias-shadow-war-against-west

[12] Cybersecurity and Infrastructure Security Agency, APT Actors Exploit Ivanti Vulnerabilities in Federal Agencies and Critical Infrastructure Organizations (AA24-241A) (2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a

[13] Office of the Director of National Intelligence, Recent Cyber Attacks on U.S. Infrastructure Underscore Vulnerability of Critical U.S. Systems (June 2024), https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

Threat Assessment Framework

The growing prevalence of cyber-attacks requires government agencies to audit and categorize these attacks to identify patterns, trends, and vulnerabilities. There is currently no large scale framework to do this. Agencies and citizens are left to only narrowly focus on individual attacks rather than attacks as a while. I propose developing a system that allows agencies to categorize cyber-attacks in an effort to shift to long term analysis. These attacks are broken up as Type A, B, and C attacks.

Type A

Type A attacks are defined as direct assaults on physical hardware. These attacks are designed to quickly disrupt, disable, or destroy critical infrastructure, often with immediate and tangible consequences. They target physical components essential to communication, energy, transportation, or military operations. The sabotage of undersea cables, for example, would fall into this category. Severing these cables could cause widespread internet outages and economic disruptions. Other examples include attacks on power grids, server farms, or telecommunications towers, where physical damage could lead to cascading failures in connected systems.

Type B

Type B attacks are defined as attacks that exploit software vulnerabilities and involve cyber intrusions. These attacks occur when a bad actor gains unauthorized access to a system to steal, manipulate, encrypt, or corrupt data. They can range from sophisticated nation-state cyber operations to ransomware campaigns targeting businesses and governments. A successful Type B attack could involve exploiting vulnerabilities to compromise critical software, injecting malicious code to create backdoors, or launching denial-of-service attacks to overwhelm systems. The impact of these attacks can extend beyond simple data loss, and could lead to shutdowns, financial losses, and long-term national security risks.

Type C

Type C attacks are hybrid complex attacks. These attacks have multiple intersecting components, making them more difficult to detect, defend against, and recover from. They are a mixture of physical attacks, software exploitations, and other methods combined to maximize disruption. The "other methods" often include political and related misinformation campaigns designed to spread fear and distrust after an attack, further destabilizing the target.

A hypothetical attack of this nature would look as follows: A non-state actor targets election infrastructure, deploying ransomware on numerous related systems to encrypt critical voter databases and disrupt election processes. At the same time, the bad actor launches a targeted misinformation campaign. Using formats such as social media or fake news articles to either cover up the issue or deepen political tensions. This could involve spreading false claims that the election was rigged, that certain votes were lost or manipulated, or that government agencies are suppressing the truth. By combining cyberattacks with psychological warfare,

Type C attacks create chaos, and weaken public trust.

Most exsisting analysis of cyberattacks focus on the short-term effects of said attack. Generally, these frameworks do not connect attacks long term. This framework helps to categorize attacks in a way that helps agencies apply a type and track any patterns or trends. This framework emphasizes the need to shift the perspective of cyberattacks to a possible long-term degradation of our critical infrastructure. This framework will also allow agencies to group together various attacks. By assigning these designations, attacks can be easily grouped together and analyzed more efficiently.

Policy Recommendations

Further from developing this framework, there are policy decisions that must be made. It is the responsibility of the government to take threat of attack on our critical communication infrastructure seriously. Lawmakers can better equip the U.S to prepare for cyberthreats to our critical communication infrastructure by expanding federal oversight to better prevent, respond, and analyze cyber threats, and developing an alternative communication network via satellite mesh networks.

Federal Oversight

One of the most effective ways to mitigate cyber threats to the U.S. communication infrastructure is through stronger federal oversight and increased coordination effort between the government and the private sector. Agencies like CISA should establish stricter security standards for telecom providers, ensuring that cybersecurity is a top priority for critical infrastructure. CISA should set standardized security system requirements, mandatory reporting of cyber incidents, and rigorous compliance checks. Additionally, federal oversight should emphasize intelligence sharing. This will help us to quickly come to conclusions about cyber-attacks as well as find innovative solutions. CISA should also collaborate closely with the National Institute of Standards and Technology (NIST) to develop and implement even stricter cybersecurity frameworks.[15]

The private sector owns and operates most of the the nation’s communication infrastructure, making its involvement essential in executing these measures. By integrating private companies more deeply into the policy-making process, the federal government can create practical, effective security standards that account for real-world industry challenges. Intelligence sharing must also extend to these private entities, as they are prime targets for cyberattacks and often possess valuable insights into emerging threats.

Increased reporting is another critical component in detecting and preventing cyberattacks. These reports enhance transparency, facilitate better risk assessment, and enable a collective approach to cybersecurity by incorporating shared insights and analyses across multiple organizations. Strengthening these reporting mechanisms ensures a more proactive defense against cyber threats.

---

[15] H. Riggs et al., “Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure,” Sensors 23, no. 8 (2023): 4060, https://doi.org/10.3390/s23084060

Satellite Mesh Network

Another key recommendation is creating a backup communication network that operates separately from traditional internet and cellular networks. If an attack were to disrupt these primary systems, a secondary network could keep critical services online. Establishing such a network is crucial to ensuring that communication remains functional even in the event of a large scale cyberattack.

An emergency network can be created using a Satellite Mesh Network. This network has been tested and used by the military, but not beyond that. Most satellite networks rely on transition between devices and a singular satellite. The Satellite mesh network utilizes multiple satellites all calibrated on a Peer-to-Peer network.[16] This means that all satellites function the same meaning that if one goes down, the network will remain online. This method also utilizes readily deployable ground transceivers referred to as nodes. These nodes act in a similar manner to satellites where if one goes down, the network will remain online.

A network of this nature would be critical and effective should regular networks fail due to a cyberattack. They are easily deployable and easily calibrated to provide quick relief. This network is also very resilient in its redundancy of all satellites and nodes functioning interdependently. There are certain limitations pertaining to cost, and the implementation of infrastructure, however the necessity is there.

A case study conducted by Silvus technologies in the Florda Key's demonstrated the effectiveness of this strategy should the need arise. In this case study they demonstrated how simply this network could be set up. This test linked an emergency operations center, a mobile team, and the satellite network. They then connected a handheld radio to the network to show its versatility for communications on the go.[17]

Conclusion

A thorough analysis of our critical communication infrastructure shows that we are dangerously unprepared to confront cyber threats. These threats are imminent, evolving, and capable of inflicting catastrophic damage. It is imperative that we take decisive action now to prevent and mitigate future disruptions.

The case studies are evidence that our vulnerabilities are not just theoretical concerns but have happened and caused significant harm. Large-scale breaches compromising sensitive data and targeted attacks crippling essential services are extremely dangerous. Without proactive intervention, we are leaving ourselves exposed to threats that could dismantle systems that we use every day. Ignoring this risk would be gross negligence and jeopardize the security of our nation.

To close the gaps in our preparedness, we must implement practical executable solutions. Expanded federal oversight, along with the development of an alternative communication network, like the proposed Emergency Satellite Mesh Network, would provide critical redundancy in times of crisis. Both solutions provide both preventative and reactive solutions to respond to any type of cyber threat.

---

[16] Silvus Technologies, Transpondr Emergency Management (2020), https://silvustechnologies.com/wp-content/uploads/2020/01/Transpondr-Emergency-Management.pdf

[17] Silvus Technologies, Transpondr Emergency Management (2020), https://silvustechnologies.com/wp-content/uploads/2020/01/Transpondr-Emergency-Management.pdf.

Most importantly, we should reframe our understanding of cyber-attacks. We have for too long treated them as singular short-term events like earthquakes. But this type of thinking is flawed. Cyber threats are more like wildfires. They are dangerous and destructive and can spread to uncontrollable sizes. Just as multiple small wildfires can turn into a massive fire, individual cyber-attacks can ignite widespread systemic failure.

Strategic Misperception and Great Power Security Competition

Chick Edmond

ABSTRACT

The author of this article contends that current great-power rivalry is largely based upon non-material factors that result from interactions of mistrust, misperceptions and misunderstandings, rather than changes in material capability. Building upon advancements in behavioral geopolitics, network theory and security-dilemma research, the article presents a comprehensive model of how cognitive biases, structural inequalities and institutional degradation contribute to escalation risk, although neither side intended it. The author demonstrates that as states gain more power, they become more afraid of their less powerful rivals, leading to preventative measures that seem irrational to outsiders; however, those same measures can make rational sense inside each respective country's cognition. In addition, the author presents a new term — the Business Security Dilemma — to demonstrate how these issues move beyond state-to-state interactions to incorporate multinational companies and global supply lines; thereby creating instability due to increased reliance upon interdependent economies. Ultimately, the author argues that achieving mutual understanding (a long-standing goal of diplomacy) may be impossible because of structural differences among countries' strategic cultures, history, and internal politics. Therefore, instead of focusing solely on achieving mutual understanding, there needs to be a greater emphasis placed on establishing rules and procedures for communicating during crises as well as developing mechanisms for preventing escalations that will continue regardless of any level of misperception.

Keywords: strategic misperception, security dilemma, great power competition, behavioral geopolitics, weaponized interdependence, conflict escalation

Introduction: The Return of Fear

Fear is the primary motivator for Athens and Sparta entering into conflict, according to Thucydides' (as cited in Acemoglu & Wolitzky, 2024), when writing of the Peloponnesian War. He writes "what made war inevitable," was "the growth of Athenian power and the fear which this caused in Sparta" (Thucydides, 2003). Nearly two thousand years after his writings, it is still surprising that today's international relations demonstrate many of the same characteristics. Today, we find ourselves in a new age of great power rivalry — an age of rivalry driven by misinterpretation of each other's intentions, capabilities, and limits.

Evidence supports this assessment. The U.S. and China have developed a self-reinforcing cycle of misperception. For every single instance where China uses its aircraft carriers during large-scale regional maneuvers, China characterizes them as routine training and defensive in nature. On the other hand, U.S. Defense Secretary Pete Hegseth has stated that the United States is ready to fight and win against China. To Beijing, this represents a signal that Washington is preparing for preemptive action (Bridoux, 2017). Both sides are not intentionally lying; both parties are interpreting events based upon their genuine beliefs. There exists an underlying difference in worldview regarding legitimate security behaviors and international order.

The 2025 US National Security Strategy has codified this change. In essence, the strategy declared the end of the post-WWII Pax Americana. It called for "fair" and "reciprocal" alliances while signaling a strategic

shift away from global commitments. More significant was the way the strategy treated adversaries. China was described primarily as an economic competitor versus a full-scope strategic competitor, while Russia was no longer characterized as a top-tier threat to the U.S. despite continuing to wage war in Ukraine (Hayat & Khalil, 2020). However, neither Beijing nor Moscow has taken the signals contained within the National Security Strategy to indicate a decrease in aggression. Rather, both countries view these changes as signs of weakness/decline and opportunities for further expansion.

This paper argues that strategic misperception is not simply a communications problem that will be solved by better dialogue — it is a systemic issue created by the interactions of three analytically independent elements. First, distrust creates worse-case thinking, which increases threat assessments. Second, misperception leads states to act on what they perceive their opponents have done, rather than what they have actually done. Lastly, misunderstandings create conflicting higher-order beliefs that will continue even if there is no additional data collected (Acemoglu & Wolitzky, 2024).

All of these issues are compounded by findings in behavioral geopolitics research demonstrating a seemingly counter-intuitive relationship between power and fear. Research demonstrates that greater power levels lead to greater fears of less capable competitors. A study of Russian elite attitudes toward the United States and NATO found that Russian elites who believed Russia possessed greater military capability than did their peers had greater fears of all three actors, including neighboring Ukraine. No other psychological or demographic variable contributed to increasing perceptions of Ukraine as a threat to Russians more than greater perceptions of Russian military capability (Kirilova, 2024).

Similarly, studies examining U.S. diplomatic cables from the Cold War period show that those U.S. government officials who expressed a greater sense of U.S. global military power viewed the Soviet Union, China and Viet Cong as larger threats than those who were less confident in America’s relative strength (Zhang, 2023).

In terms of implications for international order, the consequences are far-reaching. Given that strategic misperception is a structural feature of the current system of international relations rather than an

incident-specific phenomenon, relying solely on traditional methods of preventing conflict such as enhanced communication, confidence building measures, and diplomacy are insufficient. Instead, what is needed is a paradigmatic shift in our understanding of how great powers interact in times of uncertainty; specifically, an

acceptance that achieving mutual understanding is unlikely and therefore the focus should be on creating competitive environments with reduced potential for catastrophic escalation.

This article consists of five sections. Section 2 develops the theoretical framework using recent developments in analyzing mistrust, misperception and misunderstanding combined with traditional security dilemma theory. Section 3 provides examples of how structural differences in global networks transform economic interdependencies from being pacifying forces into areas for strategic coercion, introducing the business security dilemma. Section 4 discusses the behavioral aspects of perceiving power — using recent research in political psychology — explaining why dominant powers consistently perceive threats from weaker competitors at much higher levels than they actually exist. Section 5 addresses implications for preventing conflicts by developing institutional frameworks that operate independently of misunderstanding, thereby reducing the risk of escalating violence.

An integrated model of mistrust, misperceptions and confusion

The study of conflict between countries has identified a number of reasons why countries fight, including that all countries operate under some degree of uncertainty regarding other nations. Recently, there has been significant advancement of the understanding of how the three types of uncertainties -- mistrust, misperceptions and confusion - work together to drive conflict.

The three types of uncertainty

Mistrust refers to uncertainty about another country's objectives or capabilities. It is perhaps the most well-known form of uncertainty related to international conflict. For example, does China really support the status quo in Taiwan or does it want to revise the current status quo? Is the U.S. committed to defending its allies in Asia during times of crises? These are difficult questions to answer because nations often want to conceal their true interests and can exaggerate their capabilities.

Formally speaking, mistrust relates to incomplete knowledge about an opposing nation's type and therefore resembles many models of adverse selection and screening (Acemoglu & Wolitzky, 2024). The classic security dilemma demonstrates this relationship. Although two countries may wish to avoid going to war at all costs, if they do not know which type the other is (e.g. whether they are capable of choosing the war option), they may feel compelled to build weapons or engage in aggressive behavior to protect themselves against being attacked first. The ambiguity surrounding the U.S. stance toward Taiwan in the 2025 National Security Strategy - the policy acknowledges China's claims to Taiwan but also maintains that the U.S. is obligated to provide security assistance to Taiwan - represents how mistrust creates a worst-case scenario for both countries.

Misperceptions refer to the inability to see what another nation does. Countries sometimes do not observe what their rival nations do. A naval exercise designed as a routine training exercise may appear to be a provocative demonstration of force. A defensive alliance may appear to be an offensive coalition. A conciliatory gesture may be seen as a sign of weakness by an adversary who believes that such weakness invites him/her to exploit that vulnerability.

Although theories of conflict have devoted much less systematic consideration to misperception than to mistrust, misperception is just as important. The U.S. Navy's Freedom of Navigation Operation (FONOP) program illustrates this point. Each year China routinely interprets FONOP as "provocative military activity" demonstrating "gunboat diplomacy." On the other hand, the United States consistently interprets FONOP as "routine naval activities" that uphold international maritime law. While each side genuinely believes in its respective interpretation, the actual conduct of naval exercises by both sides appears virtually indistinguishable (Zhang, 2023).

Misperceptions can create greater potential for increased conflict levels than either mistrust or misunderstanding because when misperceptions occur regularly between states, those states tend to react not based upon what the rival nation has done but rather based upon what they believe the rival nation did.

Therefore, when perception discrepancies develop between states on a regular basis, conflict can escalate even if none of the parties involved intend it to escalate.

Misunderstandings represent the least understood and likely most dangerous form of uncertainty. Misunderstandings refer to uncertainty regarding what an adversary believes concerning one's own actions or intentions (i.e. second order beliefs). Do China and the United States believe that China understands that the U.S. sees its naval exercises as defensive? Do China and the United States believe that each understands that the other views FONOP as provocation? When second order belief differences exist between states, they

may engage in actions believing that those actions will be interpreted as conciliatory but instead find that the adversary interprets them as escalatory.

Nancy Pelosi's trip to Taiwan in August 2022 represents a good example of misunderstanding. The majority of Americans believed her trip represented a continuation of the status quo and therefore was a benign act. On the other hand, China saw it as an important escalation. Similarly, when Chinese Defense Minister Wei Fenghe said he would fight "to the last man" should Taiwan declare independence, America interpreted his words as an escalation whereas China argued that he was simply stating that China would continue to enforce its position regarding Taiwan as per the existing status quo (Wang, 2019). In both cases, each country's interpretation was genuine but systematically contradictory.

The Security Dilemma Revisited

John Herz developed the concept of a "security dilemma" to describe the process where one country takes action to improve its national security which ultimately decreases the national security level of its rival(s). As Herz wrote, "the essence of the security dilemma... lies in the fact that increases in one country's security level lead inevitably to decreased levels of security for neighboring countries" (Herd, 2010). Robert Jervis expanded this idea when he explained that states have difficulty determining whether the actions taken by an enemy are meant for offense or for defense purposes (Jervis, 1978). He explained further that since states do not have reliable methods for making such distinctions, when states attempt to increase their national security levels, they often inadvertently increase the security threat levels for other nations.

Building upon this basic premise, (Acemoglu & Wolitzky, 2024) explored how mistrust, misperceptions and misunderstandings combine and separately affect conflicts between countries. In a one-time interaction model of a security dilemma involving only mistrust-based uncertainty between two states, if each state assigns a sufficient level of risk to the possibility that its rival is a "bad-type" who will always opt for warfare, then even states that truly prefer peace will engage in arming, preemptive attacks before their rivals.

However, once interactions between states are extended over time, additional complexities emerge. Specifically, if states misinterpret peaceful actions as hostile and/or aggressive actions, then misperceptions can cause a conflict spiral that can persist for extended periods and result in widespread conflict, regardless of whether or not either state actually wants conflict.

Finally, misunderstandings, defined as differences in what states believe about their opponent's observations regarding past events/actions, can result in permanent conflict traps. Such misunderstandings can persist indefinitely after conflicting interpretations have formed, e.g., China continues to perceive U.S. Freedom of Navigation Operations (FONOP) as "provocative military activities"; similarly, the United States continues to perceive FONOP as "standard naval operations" that comply with international maritime law. Since each side observes every action taken by the other side through lenses created prior to any particular action and has limited ability to determine what private interpretations its opponent holds, neither side alters their perceptions (Acemoglu & Wolitzky, 2024).

Weaponized Interdependence and the Business Security Dilemma

As we see a similar dynamic at play in the economic sphere as strategic misperception fosters the growth of great power rivalry on the traditional security side; a parallel dynamic is developing on the economic side. What is perhaps the greatest single development in modern international relations is the evolution of global economic networks from being areas of mutually beneficial relationships to becoming venues for strategic coercion.

From Complex Interdependence to Weaponized Networks

Farrell and Newman (2019) first described the idea of “weaponized interdependence” as describing the ability of states to utilize their control over global networks to pursue strategic goals. Farrell and Newman’s central insight is that global economic networks are not flat, decentralized structures of mutual dependence, but rather are centralized systems where a small number of nodes function as critical hubs. States that control these hubs – whether by virtue of having jurisdiction over the companies operating on them, or through regulatory means – possess significantly more power than their size in the markets would suggest.

SWIFT, a major clearinghouse for electronic funds transfers around the world, serves as a good example of this type of relationship. Because SWIFT plays a central role in facilitating the flow of money internationally, it also facilitates the collection of information regarding almost all international monetary transactions. Following the September 11th terrorist attacks, the U.S. government gradually turned this source of data into a tool for surveillance and then later used it as an instrument for diplomatic coercion. In 2012, combined actions taken by the U.S. and E.U. forced SWIFT to remove Iranian banks from its network. According to a former executive of SWIFT, "Disconnecting banks is an exceptional and previously unexplored measure for SWIFT. It is a result of the collective effort of international and multilateral actors to increase financial sanctions imposed upon Iran" (Farrell & Newman, 2019, p. 27).

Semiconductors represent the focal point for this new form of economic warfare. U.S. trade restrictions against Chinese firms such as Huawei and SMIC limit their access to cutting-edge semiconductors that are essential for use in both civilian and military products. These trade restrictions were intended to delay China’s advance toward achieving parity with the U.S. in terms of technological capabilities and protect America’s competitive advantages (Scobell, 2020).

The Business Security Dilemma

While Farrell and Newman’s conceptualization of “weaponized interdependence” addresses primarily state-level behavior, they leave unanswered questions concerning how firms and third-party states act in response to competing great powers’ pressure. Mazarr, (2022) addressed this gap with their introduction of the “business security dilemma,” drawing parallels between states facing a security dilemma in their strategic interactions and firms located in third-party states who confront a comparable dilemma due to conflicting pressures from the United States and China.

At issue here is the fact that firms’ security alignment with the United States was found to be the primary explanatory variable for cooperative behavior among firms relative to compliance with U.S. export controls

— exceeding even economic power or business interest factors. Through case studies involving South Korea, Taiwan, Germany, and the Netherlands, Popescu, 2025 demonstrated that third-party governments with greater security alignments with the United States (Taiwan and South Korea) displayed greater levels of cooperation compared to those governments with lesser security alignments (Germany and the Netherlands).

This finding contradicts arguments suggesting that high-value businesses dependent on the dominant power or indirect reliance by firms on the targeted state drive cooperation. TSMC and Samsung, two companies that have extensive economic connections to China and whose businesses depend heavily on the Chinese market, have largely cooperated with U.S. export controls because their respective home governments’ security alliances with the United States take precedence over economic interests (Oluyemi, 2025).

The Business Security Dilemma expands the scope of the security concept beyond the interstate level into the domain of multinational corporations. Cooperation by firms with U.S. export controls may lead to retaliatory measures by China against these firms, potentially limiting their future market access.

Conversely, non-compliance with U.S. export controls may subject these firms to penalties under U.S. law, thus potentially jeopardizing their access to key technologies. In neither case does there exist a low-cost option for firms that wish to avoid being drawn into a cycle of increasing obligations from both sides.

The Digital Domain

A third area in which strategic misperceptions converge with weaponized interdependencies exists in cyberspace. Following five years of negotiation, a permanent UN mechanism for addressing cybersecurity was finally established. However, unlike what occurred at NATO during the Cold War, where Washington could rely upon emerging powers to support it against Moscow or vice versa today; emerging powers — India, Indonesia, Brazil, and South Africa — instead developed positions emphasizing their developmental needs vis-a-vis competition between Washington and Beijing (Hayat & Khalil, 2020).

These "emerging powers," therefore, experience a singular burden — advancing their foreign policy influence abroad while meeting pressing domestic needs including poverty reduction, health care delivery improvements, and closing digital infrastructure gaps. This double-pressure accounts for why these countries appear inconsistent in their decision-making processes. Emerging powers are equally content purchasing 5G equipment from providers based in either Europe/USA or China (e.g., Huawei). Similarly, emerging powers are equally wary of espionage from both the Five Eyes coalition and Chinese spy operations (Hayat & Khalil, 2020).

Strategic autonomy encapsulates these countries' stance. Emerging powers do not need to choose between Washington and Beijing; they are members of every club. For instance, India collaborates with Washington on tech security via the Quad while collaborating with Beijing/Russia in BRICS on digital economy matters. Likewise, Indonesia participates in both Washington-sponsored IPEF and Beijing-friendly BRICS groups on digital economy issues. Emerging powers thereby enable themselves to purchase the best possible deals available on tech-transfer investments/donor-assistance aid from both camps without ideological considerations (Mazarr, 2022).

Thus, we observe a structural shift occurring in global competition. On one hand, American strategies — as well as those employed by China — assume that ultimately all emerging powers will affiliate themselves

with either Washington or Beijing. Yet emerging powers are establishing their own coalitions frameworks and diminishing Washington's/Beijing's influence on creating global standards/rules (Basu, 2025).

The Behavioral Geopolitics of Power Perception

If we recognize that misperception is structural, then it becomes vital to determine how perceptions of power affect our ability to understand. In recent years, a growing body of research has emerged in the field of behavioral geopolitics. The researchers in this area apply insights from political psychology to international relations to identify and explain a series of counterintuitive behaviors that contribute to modern escalatory dynamics.

How Power Affects Perceived Threats

Recent research by Caleb Pomeroy regarding the effects of power on thinking and behavior of business leaders provides a strong basis for understanding the processes of international policymakers. The research indicates a wide variety of behavioral patterns. Powerful individuals tend to begin arguments in debates or negotiations. This approach tends to give them a significant advantage. However, powerful individuals also rely upon stereotypes and discount the opinions of others, which can cause them to dismiss critical information when making decisions (Popescu, 2025).

When problems increase in complexity, policymakers rely more upon what Nobel Prize winner Daniel Kahneman referred to as “System 1 Thinking,” i.e., rapid, intuitive decision-making using heuristics, emotions, and experience as opposed to careful deliberative consideration. An important drawback to System 1 thinking is that it often causes policymakers to fear challenges. The response to criticism triggers natural fight-or-flight reactions, causing a perception of attack without an opportunity for rebuttal (Popescu, 2025).

These findings are applicable to foreign relations. Survey data of Russian elite policymakers demonstrate that those policymakers who believed Russia was more powerful than did the average respondent, reported feeling threatened not only by the United States and NATO but also by their neighbor, Ukraine. There is no other psychological or demographic variable that caused respondents to report feeling threatened by Ukraine as a result of Russia’s perceived power to the extent of the perceived strength of Russia (Scobell, 2020).

This finding is counterintuitive: one would logically assume that those who believed their countries were stronger than their adversaries would report feeling less threatened by weaker neighbors. Rather, it appears that power generates fear.

Cold War-era U.S. State Department diplomatic cable analyses reveal comparable findings. U.S. diplomats and politicians who exhibited a stronger sense of U.S. global power reported perceiving the Soviet Union, China, and the Viet Cong as larger threats than those who displayed more restraint in their assessment of

U.S. global power. These patterns existed throughout multiple presidential administrations and geographic areas, indicating that they reflect a common psychological phenomenon rather than a function of particular

historical events (Gulf Times, 2026).

The Escalating Effects of Preventive Action

If power generates fear and fear produces perceptions of threat, then the next reasonable conclusion is preventive action. When powerful nations perceive threats from weaker rivals, they may use force to neutralize those threats prior to their manifestation. For outside observers, these uses of force may seem illogical – why would the world’s greatest power perceive a much weaker competitor as threatening?

However, within the context of the cognitive framework of power, such uses of force represent not only rational but necessary actions.

This dynamic explains several recent events. The Russian full-scale invasion of Ukraine in 2022 was motivated by neither territorial acquisition nor expansion. Rather, it was intended to prevent Ukraine from continuing to develop closer ties with Western organizations that Russia views as existential threats (Posen & Ross, 1996).

Similarly, the U.S. military raid on Venezuela in January 2026 that captured Venezuelan President Nicolás Maduro on narcotics-terrorism charges exemplified a preventive logic. Removing a hostile government before it solidifies its opposition to the U.S. aligns with a long-standing strategy employed by all great powers (Hayat & Khalil, 2020).

Finally, although likely not successful in achieving its objectives, the U.S.’ coercive pressure applied toward acquiring Greenland reflects the same underlying mechanism. As climate change makes parts of the Arctic more accessible and as Russia and China continue to strengthen their positions in the region, U.S. strategists view control over Greenland as indispensable for preserving strategic superiority. The U.S. willingness to suggest that action will be taken “whether they like it or not” is reflective of the same pattern of behavior described in the literature: power generates both fear and a belief that preventive action is warranted (Hayat & Khalil, 2020).

The Spheres of Influence Conceptual Framework

The 2025 National Security Strategy's revival of the concept of "Spheres of Influence," represents an institutionalization of this conceptual framework's behavioral implications. According to this framework, there are three main regions in the international system: the Western Hemisphere, Europe, and Asia. The United States asserts its dominance in the Western Hemisphere and expects its European allies to bear greater responsibility for their own security. The U.S.' interactions with Asia are limited largely to its alliance systems (Mazarr, 2022).

According to Russia and China, however, this framework serves as justification for pursuing their own "spheres of influence." Since the U.S. asserts its dominance in the Western Hemisphere, why shouldn't Russia assert its dominance in its "near-abroad?" Similarly, if the U.S. is willing to accept a trilateral division of the world, why shouldn't China assert its dominance in the South China Sea and beyond?

A primary risk associated with accepting spheres-of-influence thinking is that it can become

self-reinforcing. When the U.S. signals that it will not challenge Russian actions in Ukraine or Chinese actions in the South China Sea, it may perceive this as acceptance of its own dominance in the Western Hemisphere. Conversely, for revisionist powers, such signals may be perceived as examples of weakness or passivity and serve as encouragement for additional aggression (Wang, 2019). This describes a classical example of the spiral model operating at a grand-strategic level.

Controlling Escalation: Moving Beyond Conflict Prevention

If we correctly assess that strategic misperception is structural; that power generates fear; and that weaponized interdependence develops new pathways for escalation; then we must revise longstanding approaches to conflict prevention dramatically. The idealistic notion of achieving mutual understanding via diplomacy may be unrealistic. Instead, we must seek ways to manage the negative consequences of unavoidable misperception.

Why More Effective Communication Will Not Solve the Problem

We are tempted to advocate for improved communication between parties in conflict. It seems obvious that if both sides had clearer intentions for their respective actions, we could minimize misperceptions. However, history contradicts us. The United States and China have engaged in extensive communication for decades. They have established numerous bilateral dialogues and working groups as well as formal exchange programs since normalizing relations in 1979. Nonetheless, misperceptions have not decreased; in some cases, they have actually worsened.

There are several reasons why improved communication cannot resolve these structural misperceptions. First and foremost is the distinction between technical misunderstandings and structural disagreements. Technical issues can generally be resolved through discussion. Structural disagreements regarding international order remain after prolonged diplomatic engagement (Herd, 2010). China and the United States do not misunderstand each other’s positions on Taiwan or the South China Sea; they understand each other's positions fully and fundamentally disagree (Acemoglu & Wolitzky, 2024).

Secondly, nuclear dimensions multiply misperception risks. Dual-purpose ambiguities created by carrier operations proximate to nuclear-capable missile bases complicate communications between rival states during times of tension; what may initially appear as preparations for a conventional operation may be interpreted as preparatory activities for a nuclear strike (Wang, 2019).

Additionally, nuclear dimensions reduce available timeframes for resolution during crises; therefore, communicators face an impossible dilemma between acting quickly enough to avoid miscalculation versus developing sufficient clarity regarding intentions (Oluyemi, 2025).

Thirdly, communication styles employed by policymakers can impact interpretations of messages sent by counterparts. Direct rhetorical style employed by the Trump Administration intended as deterrence is

commonly interpreted by Chinese analysts as representative of aggressive postures rather than defensive stances (Oluyemi, 2025).

Research supports this interpretation: Seven years of Freedom of Navigation Operations (FONOP) have led China to transition from "cautious rejection" of U.S. messages towards more explicitly hostile responses (Zhang, 2023).

Developing Systems That Can Operate Successfully Regardless of Miscommunication

If we acknowledge that miscommunication cannot be eradicated completely, then we must redirect our efforts towards mitigating its negative effects. We propose four practical steps to mitigate escalation risks while recognizing the persistence of miscommunication:

Firstly, establish a 24-hour crisis hotline process modeled on precedent set by U.S.-USSR contacts during the Cold War. Independent channels for military-to-military communications must exist regardless of diplomatic tensions existing between states; when carrier groups inadvertently cross paths during naval maneuvers professional naval personnel must have direct contact channels available - not bureaucratic delay (Zhang, 2023). Experience from previous instances illustrates the value of such independent communication channels during periods of heightened tension: Examples include preventing miscalculations occurring during both the Cuban Missile Crisis and 1973 Arab-Israeli War (Zhang, 2023).

Secondly, negotiate an exercise notification agreement requiring advance notification prior to conducting large-scale naval operations beyond the second island chain (e.g., Guam). While such an agreement would not remove possible misinterpretation regarding motivations behind such operations -- it would decrease unexpected encounters allowing participating parties to prepare responsive measures (not reactionary) prior to encountering provocative forces (Lowy Institute, 2025). ASEAN's current attempts to negotiate a South China Sea Code of Conduct with China presents an example of a regional framework for implementing such mechanisms (Zhang, 2023).

Thirdly, we need to develop separate nuclear and conventional signaling systems along with shared protocols for de-escalation when there is an incident involving carriers. Dual use ambiguity – where routine conventional exercises could look like preparations for a nuclear strike – presents the greatest risk of escalating into a full-blown conflict. Establishing clear protocols to distinguish between conventional and nuclear military activities would likely decrease the number of times routine exercises are mistaken for nuclear alert signals (Zhang, 2023).

Fourthly, create quarterly Track 1.5 interpretation forums focused on explaining one side’s strategic rationale to the other instead of attempting to alter its strategic rationale. Actors in the region such as Singapore and Malaysia, which have maintained relatively balanced relationship with both superpowers, can host these forums as they offer a neutral forum over which neither Beijing nor Washington has control (Zhang, 2023).

5.3 Role of Third Parties

The analysis of emerging powers' strategic autonomy also indicates that third parties will continue to perform critical functions in facilitating management of great power competition. For example, countries such as India, Indonesia, and Brazil do not seek to identify themselves exclusively with either the U.S. or China but instead pursue their own individual trajectories. Given that they remain capable of maintaining bilateral relationships with both the U.S. and China while also developing their own interests, they may serve as valuable facilitators in crises (Farrell & Newman, 2019).

Although the EU has experienced significant challenges in developing its relations with both the U.S. and China, its experiences provide important lessons. The EU's ability to maintain positive economic engagements with China while working together with the U.S. regarding technology security demonstrates a pragmatic model that emerging powers may follow. Additionally, the EU's articulation of "strategic autonomy," i.e., the capability to act autonomously within its alliances, resonates with the orientations of emerging powers (Kirilova, 2024).

For the U.S. government, the implications are clear. Rather than viewing emerging powers as prize assets to be secured through zero sum competition against China, policy makers should view emerging powers as potential allies possessing their own valid interests. Therefore, policy makers should focus on practical cooperative actions among emerging powers related to supply chain security; capacity building; and technical standards — as opposed to requiring that they adopt ideologically aligned positions. In fact, Popescu (2025) contends that "the most effective strategy…focuses on practical cooperation in areas like supply chain security and technical standards — as opposed to demanding ideological alignment."

Conclusion: Competition Without Catastrophe

In conclusion, this study has made the case that today's great-power competition is fundamentally defined by structural misperceptions which will never go away no matter how much better we communicate and understand each other. Misunderstanding, mistrust, and misperception combine to create an escalating dynamic neither side can control, nor even entirely intend. Research on behavior suggests that power generates fear among those holding the upper hand; thus, powerful states are inclined to view weakness in others as a threat and take preventive action against them that looks unreasonable to outsiders but makes perfect sense to insiders.

Global networks have also evolved over time to transform what were once mutually beneficial relationships into strategically coercive ones. The business security dilemma illustrates how companies and countries acting as third parties find themselves ensnared in spirals of conflicting demands that could lead to escalations whether they want it or not. The digital world adds new layers of uncertainty as rising powers seek strategic independence rather than alignment with either Washington or Beijing.

That being said, the future does offer some cause for cautious optimism. As previously noted, the same structural forces generating misperception can be managed by designing institutions. There are several

hotlines, notice of exercises, separate communication channels for nuclear and non-nuclear operations and Track 1.5 interpretation forums can all help to mitigate the risk of escalations without necessarily requiring mutual understanding. We now know from our Cold War history that it is possible to have great power competition without catastrophic war, even if adversaries do not trust one another.

It is essential to repeat again: the objective is not to achieve mutual understanding – which might be impossible due to structural differences regarding international orders — but competition without war. To reach that objective, one needs to accept that misperception is permanent and therefore make it less

hazardous. In terms of success, we should measure it not by reduced misperception – which is impossible — but by a reduction in crisis escalation time from hours to days and still maintain deterrence credibility (Wang, 2019).

As the United States, China and Russia move forward in navigating the new landscape of strategic competition, the greatest danger would be to continue treating misperception as a communications issue instead of recognizing it as a structural issue. Conversely, continuing to think that improved communication will solve basic disagreement will likely result in the same kind of catastrophe that Thucydides described over two thousand years ago: wars caused not by a rational consideration of self-interest but by the fear generated by power in those possessing it and those confronting it.

References

Acemoglu, D., & Wolitzky, A. (2024). Mistrust, misperception, and misunderstanding: Imperfect information and conflict dynamics. In Handbook of the Economics of Conflict (Vol. 1, pp. 59-104). Elsevier.

Bridoux, J. (2017). Stronger than strong: Perceptions and misperceptions of power. In American hegemony and the rise of emerging powers (pp. 19-39). Routledge.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International security, 44(1), 42-79.

Hayat, M. Z., & Khalil, M. T. (2020). Great Power Competition and Global Strategic Stability. CISS Insight Journal, 8(1), P01-27.

He, K. (2012). Undermining adversaries: Unipolarity, threat perception, and negative balancing strategies after the Cold War. Security Studies, 21(2), 154-191.

Herd, G. P. (2010). Great Powers and Strategic Stability in the 21st Century: Competing visions of world order. Routledge.

Jervis, R. (1978). Cooperation under the security dilemma. World politics, 30(2), 167-214.

Kirilova, N. V. (2024). Regional conflict prevention and perceived power competition: six elements of power. In Analyzing Global Responses to Contemporary Regional Conflicts (pp. 252-274). IGI Global Scientific Publishing.

Mazarr, M. J. (2022). Understanding Competition Great Power Rivalry in a Changing International Order-Concepts and Theories.

Oluyemi, O. A. (2025). Great Power Competition (GPC) and its Implications on the Global Security Architecture. Canadian Social Science, 21(3), 24-39.

Popescu, I. (2025). No Peer Rivals: American Grand Strategy in the Era of Great Power Competition. University of Michigan Press.

Posen, B. R., & Ross, A. L. (1996). Competing visions for US grand strategy. International security, 21(3), 5-53.

Scobell, A. (2020). Perception and misperception in US-China relations. Political Science Quarterly, 135(4), 637-664.

Wang, W. Z. (2019). Destined for misperception? Status dilemma and the early origin of US-China antagonism. Journal of Chinese Political Science, 24(1), 49-65.

Zhang, B. (2023). Polarity and strategic competition: A structural explanation of renewed great power rivalry. The Chinese Journal of International Politics, 16(4), 383-405.

Strategic Learning: Amplifying the Soft Power of Education Through Systems Thinking

Dwayne Wood EdD & John Hunter LTC (Ret)

The views expressed in this paper are solely those of the author and do not necessarily reflect the official views or positions of the Department of Defense.

ABSTRACT

Education is increasingly recognized as a strategic tool of soft power, yet evaluation practices have not kept pace with its growing influence. This paper proposes a systems thinking-based framework for assessing the strategic impact of education, particularly within defense-affiliated institutions like the U.S. Department of Defense's Regional Centers. Drawing on concepts from contribution analysis and soft power theory, the framework reconceptualizes education as a dynamic, interconnected system that fosters legitimacy and sustainability through multidimensional engagement, cultural humility and trust, long-term relationship building, and norm diffusion. The paper introduces an evaluative rubric aligned with Kirkpatrick's model to support credible, context-sensitive assessment practices. This approach shifts discourse from whether education advances national influence to how its strategic contribution can be measured and strengthened. The proposed model invites future refinement and pilot testing across diverse geopolitical and institutional contexts.

Keywords: Soft power, systems thinking, education evaluation, contribution analysis, legitimacy, sustainability, regional centers, national security, influence strategy, Kirkpatrick model

Introduction

As global competition intensifies and traditional geopolitical boundaries become more fluid, nations are increasingly turning to non-coercive instruments of influence to shape the international environment in their favor (Amirbek & Ydyrys, 2014; Cull, 2022; Gauttam et al., 2024). Among these, education stands out as one of the most enduring and effective tools of soft power, a term popularized by Joseph Nye (2017) to describe the ability of a country to attract and co-opt rather than coerce. Through academic exchanges, joint research initiatives, cultural programs, and professional education, states project their values, build goodwill, and foster long-term relationships that enhance credibility, trust, and global strategic positioning (Charles, 2023; Desai-Trilokekar & Masry, 2022). In today's interconnected world, education serves not only to inform but to influence creating networks of understanding across sectors such as security, governance, environmental policy, and civil society (Amirbek & Ydyrys, 2014; Nye, 2005; Ostashova, 2020). Particularly in contested yet cooperative regions, education can play a critical role in fostering mutual respect, supporting peacebuilding, and enabling multilateral engagement.

The concept of education as a form of soft power is particularly salient in the context of U.S. Department of Defense Regional Centers, which serve as strategic platforms for advancing security cooperation (10 U.S.C. § 342, 2017; Lopez, 2023). The regional centers offer educational programs that bring together international civilian and military leaders to engage in dialogue on complex and often sensitive issues. Engagements are designed to foster mutual understanding, strengthen professional networks, and promote shared values. Given the diverse audiences, compressed timelines, and strategically sensitive content, regional centers are uniquely positioned to benefit from a systems thinking approach to education. By embedding systems

thinking into educational outcomes, regional centers can go beyond traditional knowledge transfer to become more effective strategic levers of influence. The proposed approach does not replace existing regional center capabilities but enhances capacity to serve as strategic levers of influence by embedding educational practices that are context-responsive, iterative, and strategically aligned.

This paper builds on earlier work that introduced a systems thinking model to education, particularly in complex environments like the Arctic, that can serve as a strategic soft power tool by fostering cross-sector integration, stakeholder engagement, and scenario-based learning (Wood, 2025). While that work emphasized adapting educational design to reflect the interdependent realities of regional contexts, this paper extends the application globally by focusing on how the U.S. Department of Defense's Regional Centers can better achieve soft power outcomes through systems-oriented education. The purpose of this exploration is to operationalize a conceptual model by proposing a practical evaluation framework that allows educators, policymakers, and program designers to assess the strategic impact of educational initiatives over time. Rather than replace traditional assessment models, the proposed framework supplements them by introducing legitimacy-building dimensions such as trust, norm diffusion, and long-term engagement that are often overlooked in conventional metrics. In doing so, this paper contributes to the growing conversation about how education can be more deliberately designed, delivered, and measured as a form of national power.

Education as a Tool of Soft Power

As articulated by Joseph Nye (2017), soft power is the ability of a nation to shape the preferences and behaviors of others through attraction and persuasion, rather than coercion or payment. Henne (2022) builds on Nye's foundational definition of soft power by introducing a more analytically rigorous framework that clarifies soft power as a diffuse tool used to integrate international collective action. Unlike hard power, which relies on military and economic force, soft power derives from the appeal of a country's culture, values, policies, and institutions (Nye, 2017). Nye (2017) argued the changing nature of the international framework has re-emphasized the use of intangible forms of power. In this context, education emerges as an instrument of soft power, fostering cross-cultural understanding, cultivating long-term relationships, and transmitting the values and norms that underpin international cooperation and legitimacy. Historically, education has been a cornerstone of public diplomacy (McNerney & Sotubo, 2024). International academic exchange programs, such as the U.S. Fulbright Program or the UK's Chevening Scholarships, cultivate personal and professional ties with future global leaders, many of whom go on to serve in positions of political, economic, or social influence (Lally, 2022). For instance, China is providing tens of thousands of scholarships to international students to study in China, with the likely aim of competing against U.S. leadership in educating future world leaders (McNerney & Sotubo, 2024). These programs are not intended to simply build knowledge, but foster trust, credibility, and familiarity with the host nation's values and political system (Ostashova, 2020). Similarly, the presence of globally recognized universities, research centers, and think tanks extends a country's intellectual reach and reinforces its cultural and ideological influence on the world stage.

Education has long functioned as a critical instrument of soft power shaping influence through higher education and professional military education (Greg, 2024; Jalili, 2015; Karadag, 2017; McLauchlin et al., 2022; Trunkos, 2021). As an illustrative case of the soft power potential of defense education, China's professional military education (PME) programs actively cultivate ties with both military personnel and policymakers. In countries such as Tanzania, Ethiopia, and Mozambique, longstanding relationships with specific Chinese military institutions have been reinforced by "deep benches" of Chinese-trained alumni now serving in influential positions across defense and government sectors (Nantulya, 2023). In defense and

security contexts, education as soft power takes a more targeted form. The example underscores the broader potential of defense education to shape long-term influence, an approach similarly leveraged by U.S. Department of Defense Regional Centers, which use education to build enduring relationships and promote cooperative security frameworks. The regional centers convene civilian and military leaders from across the globe to explore regional challenges, exchange perspectives, and develop common understandings rooted in international norms and rule-of-law principles. A systems thinking approach offers a way to enhance the coherence, adaptability, and relational depth of regional center education. By emphasizing interconnectivity, stakeholder diversity, and long-term outcomes, systems-informed strategies can help to ensure even short engagements contribute meaningfully to sustained regional influence. Rather than replacing current models, systems thinking strengthens them, enabling programs to better align with the complex, evolving contexts in which regional centers operate. By fostering cross-domain integration, stakeholder trust, and long-term adaptability, this approach enhances the return on investment of educational programs not only as successful engagement tools, but as strategically integrated platforms that generate enduring influence, cooperation, and measurable strategic value.

Amplifying Soft Power Through Systems-Based Education

While education has long been employed as a tool of soft power, it is argued that the impact can be amplified when designed and delivered through a systems thinking approach. Systems thinking, with its emphasis on interconnectedness, complexity, feedback loops, and stakeholder diversity, provides a strategic lens through which education can become not merely a transmission of knowledge, but a dynamic mechanism of enduring influence (Wood, 2025). It shifts educational experiences from one-way instruction to a mutual process of knowledge exchange and strategic alignment.

Multidimensional Engagement

One of the most powerful amplifiers of soft power in systems-based education is its capacity to support multidimensional engagement. Astleitner (2018) defines multidimensional engagement as an instructional design approach that incorporates targeted strategies such as activating prior knowledge, promoting intrinsic motivation, and supporting emotional regulation across cognitive, motivational, and social-emotional components of learning to address complex problems and deepen learner engagement. Multidimensional engagement fosters authentic learning environments by supporting multidisciplinary exploration through realistic, complex task scenarios and meaningful social interaction (Admiraal et al., 2019; Hashimoto, 2022; Mishra & Aithal, 2023). Instead of addressing learners solely through disciplinary silos (e.g., military strategy, environmental policy, governance), systems-based programs deliberately integrate these domains. As an example, learners are encouraged to understand how environmental change influences legal disputes over maritime boundaries, how Indigenous knowledge systems contribute to environmental resilience, and how security operations intersect with local governance and community wellbeing (Wood, 2025). This integrative perspective helps learners realize shared challenges and fosters a sense of collaborative ownership; key elements of soft power rooted in attraction and legitimacy.

Long-Term Relationship Building

Systems-informed educational design embeds long-term relationship-building into the very architecture of learning as a strategic priority. The systems approach compels program designers to treat every educational engagement as part of a larger strategic arc, where early trust-building and post-course collaboration are not peripheral but central to the program's long-term influence. Unlike conventional models that focus narrowly on the delivery of a single course or event, systems thinking frames education as a continuum of interconnected phases: pre-course orientation and expectation setting, immersive and participatory in-course learning, post-course reflection and application, and sustained engagement through alumni networks and follow-on collaboration (Jalili, 2015). When systems thinking is applied to this educational lifecycle, it amplifies soft power in several key ways. First, it builds continuity and coherence across engagements, reinforcing trust and credibility through consistent messaging and mutual recognition of shared goals. Crucially, this approach fosters relational depth, not just technical exchange. Graduates of systems-aware programs are more likely to maintain professional, cognitive, and even normative connections to the host institution or nation (Gauttam et al., 2024). These connections serve as soft power multipliers supporting policy alignment, promoting cooperation in regional forums, and creating durable networks of influence that extend far beyond the educational program's formal conclusion.

Cultural Humility and Trust

A further amplifier lies in the cultivation of cultural humility and trust. The term cultural humility is defined by Foronda et al. (2016) as a dynamic, ongoing process of self-reflection and growth, emphasizing humility, respect, and a commitment to addressing power imbalances in interactions with diverse individuals and communities. Cultural humility is essential because it fosters mutual respect and enables more authentic, trust-based relationships that are critical conditions for the long-term effectiveness of education as a soft power tool. By positioning learners not just as recipients of instruction but as contributors to a shared learning experience, systems-based education can reduce the perception of bias or ideological imposition (Chaban, 2024; Habashy & Cruz, 2021). This is especially important in regions where historical mistrust or geopolitical competition might otherwise frame educational initiatives with suspicion. Systems thinking promotes the idea that all stakeholders have knowledge worth sharing and that learning is co-created, thereby deepening the legitimacy of the educational experience (Lipuma & Leon, 2024) and thus its soft power impact. Soft power initiatives are often criticized for being overly transactional instruments of influence (Gauttam et al., 2024; Nantulya, 2023; Saaida, 2023); however, when grounded in principles of systems thinking and cultural humility, educational programs can foster more reciprocal and legitimate forms of engagement that strengthen long-term trust and cooperation.

Norm Diffusion

Another key mechanism is systems-based education's role in accelerating norm diffusion. Gelfand et al.'s (2024) discussion on social norms provides for a definition of norm diffusion as a multilevel process of norm emergence and spread, influenced by individual psychological mechanisms, interpersonal interactions within social networks, and broader ecological and historical factors that facilitate transmission and adoption across individuals and generations. A systems thinking approach enhances the norm diffusion process by embedding norms throughout the learning ecosystem, encouraging alignment at every level while remaining responsive to the diverse contexts in which education occurs. Because norm adoption is not linear or guaranteed (Gelfand et al., 2024), systems thinking supports ongoing reflection and feedback that strengthens norm internalization by responding to cultural and contextual variables rather than imposing one-size-fits-all models. When learners not only hear about international norms (e.g., rule of law, environmental governance, human rights) but also experience how these norms operate within and across interconnected systems, learners are more likely to adopt norms voluntarily and apply in their own professional contexts (Friman et al., 2024). Education that illustrates the interdependence of law, policy, and ethics in practice becomes far more persuasive than declarative statements of principle. Soft power initiatives are often criticized as thinly veiled instruments of influence, driven more by political or economic self-interest than by genuine collaboration (Charles, 2023; Gauttam et al., 2024; Saaida, 2023). To illustrate, China's approach has been faulted for relying heavily on propaganda and state-controlled messaging, while U.S. efforts have at times been perceived as promoting "American exceptionalism" rather than fostering authentic, reciprocal partnerships (Saaida, 2023). In contrast, when norm diffusion is supported by a systems thinking approach, it shifts from top-down transmission to participatory engagement embedding norms through culturally grounded, multilevel learning experiences that are more likely to generate trust and legitimacy.

Legitimacy and Sustainability

Legitimacy and sustainability are recognized as two essential conditions for durable soft power (Greg, 2024; Saaida, 2023). A systems approach to education creates the conditions in which legitimacy and sustainability can develop by aligning learning with real-world complexity, fostering inclusive participation, and promoting long-term adaptability. Within the proposed framework, legitimacy and sustainability are not isolated features of educational soft power, but rather emergent outcomes of educational systems that successfully integrate cultural humility, norm alignment, multidimensional engagement, and foster long-term relationships. By embracing the complexity of regional challenges and engaging learners as co-navigators within that complexity, systems-based education transforms learning into a platform for strategic collaboration that avoids perceptions of ideological imposition, a common critique of traditional soft power efforts. Instead, learning becomes a platform for strategic collaboration, where trust is built not only on what is taught, but on how learning takes place. When the process emphasizes mutual respect, inclusive dialogue, and co-construction of knowledge, it signals authenticity and shared purpose. This process-centered approach is what generates the emergent properties of legitimacy and sustainability because it fosters environments where participants feel seen, heard, and genuinely engaged, making outcomes more likely to endure and align with local realities. Furthermore, the systems approach promotes the ability of educational programs to evolve alongside shifting geopolitical, environmental, and social dynamics. The approach achieves this by using feedback, encouraging collaboration across different sectors, and focusing on flexibility instead of fixed content (Akib, 2025). As a result, programs can adjust to new political priorities, environmental changes, and evolving needs. By fostering adaptive, long-term engagement, the systems approach strengthens soft power, making it more resilient to disruption and more relevant across diverse, rapidly changing regional contexts.

Conceptual Model

The conceptual model not only guides program design but also provides a framework for evaluating the strategic effectiveness of education by identifying how educational activities contribute to relationship-building, norm diffusion, and long-term influence in support of soft power objectives. Figure 1 presents a conceptual model illustrating how a systems thinking approach can amplify the soft power impact of education by enabling interconnected, adaptive, and strategically aligned learning experiences.

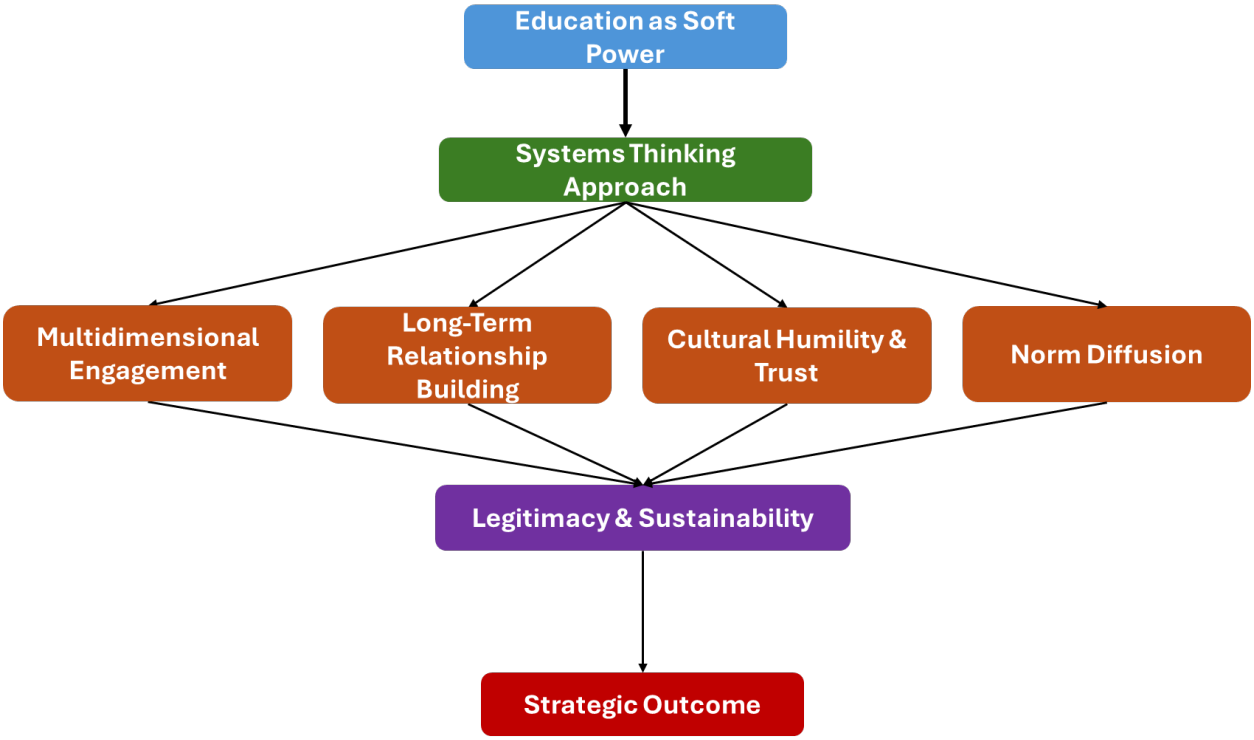


Figure 1: Conceptual model illustrating how a systems thinking approach amplifies the soft power impact of education

What makes the systems thinking framework unique as a soft power tool is its shift from viewing education as a one-way transmission of values to understanding it as a dynamic, interconnected system of influence. Traditional soft power strategies in education often focus on content delivery, transmitting culture, language, or ideology through courses, exchanges, or cultural diplomacy. In contrast, a systems thinking approach frames education as an adaptive learning ecosystem that engages multiple stakeholders, security practitioners, academics, leaders, policymakers, and scientists within a shared, context-sensitive platform. This creates a space where knowledge is co-produced, values are contextualized, and long-term trust is cultivated. As a multiplier of soft power, this approach strengthens influence through several mechanisms. First, it builds resilient, adaptive leaders who are not only informed by shared values but also skilled in navigating complexity acting as local amplifiers of cooperation. Second, it extends the impact of education beyond the learning experience by embedding feedback loops, alumni networks, follow-up engagement, and cross-sectoral collaboration to deepen and sustain relationships over time. Third, by encouraging cultural humility and systems literacy, it reduces the risk of education being perceived as ideological imposition, instead fostering mutual understanding and legitimacy. Finally, by aligning educational content with legal, diplomatic, environmental, and technological systems, it accelerates voluntary norm adoption and policy alignment. In this way, education grounded in systems thinking doesn't simply reflect soft power, it strategically operationalizes it, transforming learning into long-term, networked influence. Despite the

growing recognition of education's strategic potential, the ability to capture and measure its influence remains underdeveloped, with most existing evaluations continue to describe rather than diagnose the mechanisms through which education exerts soft power.

Descriptive Limitations in Current Soft Power Evaluation

While many scholars and practitioners acknowledge the role of education in advancing soft power, systematic approaches to evaluating its strategic impact remain limited. Some illustrative examples help demonstrate both the progress and the persistent gaps in this area. Adhikari and Saha (2023) highlight how India uses education to build soft power through university networks, international exchanges, and policy-focused think tanks but at the same time, revealing a broader challenge that the impact of education as a soft power tool remains largely descriptive. Another example of soft power evaluation is provided by Antwi-Boateng and Alhashmi (2021), who present a structured qualitative assessment of soft power in the context of the United Arab Emirates. Antwi-Boateng and Alhashmi (2021) illustrated how frameworks can help identify and organize the elements of soft power but also underscored the limitations of relying solely on qualitative analysis. Notably, Antwi-Boateng and Alhashmi (2021) acknowledge the lack of quantifiable evidence and call for more systematic, data-informed approaches to assess the tangible impact of soft power initiatives. Using a qualitative case study design, Zhu and Yang (2022) examined the experiences and perceptions of Cambodian participants in Chinese higher education programs to explore how education functions as a vehicle for China's soft power. Their findings offer further insight into this challenge by revealing that China's approach to soft power in Southeast Asia is constrained by an overemphasis on infrastructure and a lack of reciprocal educational engagement. To achieve more durable influence, Zhu and Yang (2022) argue that China must incorporate non-state actors (e.g., e-commerce platforms and tech firms), foster mutual academic exchange, and implement more sustainable and pragmatic education programs that reflect shared regional interests.

While Zhu and Yang (2022) emphasize the importance of reciprocity and relationship-building in enhancing soft power, other studies explore how educational initiatives can be evaluated for their long-term strategic value. Hong (2021) provides a case study of Australia's New Colombo Plan (NCP), a government-led outbound student mobility program designed to strengthen Australia's soft power in the Indo-Pacific region. Using an educational soft power framework, Hong (2021) evaluates the program's influence across social, cultural, and participatory capital. Hong (2021) found that while the New Colombo Plan (NCP) was effective in fostering personal relationships and cultural appreciation, the evaluation of deeper, more strategic outcomes such as participatory capital soft power remained limited. Specifically, aspects like long-term influence on host institutions and the transmission of values through student identity were not systematically captured. This case underscores the need for a more robust and long-term evaluation model, especially one that can assess how education contributes to soft power outcomes such as mutual understanding, norm diffusion, and sustained engagement.

Contribution Analysis and Systems Thinking

The examples highlight both the progress and limitations of existing soft power evaluations, particularly a tendency to focus on short-term or surface-level indicators. To move beyond descriptive approaches, emerging methodologies need to offer more holistic and adaptable tools. One such perspective provided by Thomas (2020) offers a conceptual shift by applying systems thinking to soft power, framing it not as a collection of isolated initiatives but as a dynamic, interconnected ecosystem. In this context, attempting to directly attribute specific outcomes to a single intervention such as an educational program is often neither feasible nor credible, given the complex, long-term nature of influence and the presence of multiple interacting variables. Instead, Thomas (2020) advocates for contribution analysis, which focuses on building a credible narrative supported by evidence to demonstrate how a particular initiative played a meaningful role in producing observed outcomes. A systems thinking perspective supports Thomas' (2020) concept as it reframes education as an adaptive, feedback-driven process that engages multiple stakeholders, promotes shared learning, and evolves in response to contextual changes. When designed with these principles in mind, education becomes not just a means of transmission, but a mode of transformation, supporting durable soft power outcomes through processes that legitimize, localize, and sustain influence.

While the proposed framework builds from a soft power perspective, it aligns more closely with Knight's (2022) definition of knowledge diplomacy, which reframes international education as a tool of reciprocal, collaborative relationship-building rather than unilateral influence. The emphasis on mutual benefit, co-creation, and horizontal partnerships reflects the same underlying principles embedded in the proposed evaluation framework. Moreover, the framework's emergent outcomes of legitimacy and sustainability mirror Knight's (2022) focus on durable, values-based international collaboration rather than transactional influence. By emphasizing contribution over attribution and advocating for systemic evaluation tools that capture shared norms and enduring institutional ties, the framework can help operationalize the relational ethos of knowledge diplomacy in strategic education programs. Rather than simply narrating examples of influence, the framework can provide structured data collection points and analysis methods.

Kirkpatrick Model Integration

The Kirkpatrick Evaluation Model is a widely used framework for evaluating training and education interventions (El Nsouli et al., 2023; Larasati & Asropi, 2025; Paul et al, 2024). While the Kirkpatrick model was not designed to capture strategic influence, its widespread use in educational and training settings makes it a useful foundation for expanding evaluation practices into the domain of soft power. The Kirkpatrick Evaluation Model consists of four levels with each level providing for increasing measurement of the education and training's impact. In the proposed framework, each level is reinterpreted through a strategic lens, moving from individual reaction and learning to long-term influence. Table 1 reflects a general alignment of the Kirkpatrick Evaluation Model and the proposed framework.

Table 1: Kirkpatrick Evaluation Model Levels

Kirkpatrick Level	Typical Focus	Framework	Example Data Points
Level 1: Reaction	Learners' immediate response to the learning experience	Reflects early signs of trust and cultural humility, key precursors to legitimacy	Participant satisfaction surveys
Level 2: Learning	Knowledge, skills, attitudes gained	Indicates early cognitive norm diffusion and systems awareness, foundational to later influence	Pre-/post-tests on legal or policy norms
Level 3: Behavior	Application of learning on the job or in real-world situations	Ties directly to long-term relationship building, multidimensional engagement, and the beginning of strategic soft power transfer	Follow-up interviews or surveys (6–12 months)
Level 4: Results	Long-term outcomes and impact	This is where legitimacy and sustainability emerge as soft power outcomes, beyond individual behavior, observing system-level influence	Norm adoption in policy or doctrine

Evaluation Domains & Indicators

Using the conceptual model, the evaluation framework focuses on four key domains through which soft power manifests, multidimensional engagement, long-term relationship building, cultural humility and trust, and norm diffusion. The domains reflect both the educational design principles and the observable processes that contribute to the emergent outcomes of legitimacy and sustainability. The framework is designed to be adaptable, recognizing that different education programs operate in diverse environments. Rather than prescribing fixed indicators, it offers a set of principles and examples that help practitioners identify and analyze signals of strategic impact.

Aligning Kirkpatrick's four levels with soft power indicators aids in better understanding how education contributes to influence over time. Levels 1 and 2 (reaction and learning) capture early signals such as perceived credibility, cultural openness, and initial receptivity to shared norms. The stages help evaluators assess how participants experience and internalize the learning process. In contrast, Levels 3 and 4 (behavior and results) represent deeper and more durable forms of influence, including changes in professional behavior, long-term relationship formation, and alignment with institutional or cultural values. The levels reflect the emergent outcomes of soft power that unfold beyond the learning experience. To further guide the analysis, the evaluation framework is organized into four interrelated domains (multidimensional engagement, cultural humility and trust, long-term relationship building, and norm diffusion) each representing a distinct but complementary aspect of how education functions as a strategic tool for influence and cooperation. Further, the proposed framework draws on and integrates insights from Hong's (2021) educational soft power evaluation that provides a lens to identify how education builds influence through social capital, cultural exchange, and participatory engagement. Complementing this, Knight's (2022) concept of knowledge diplomacy reinforces the importance of mutuality, reciprocity, and collaboration as guiding values for international education initiatives. Together, the perspectives help ground the framework in both practice and normative aspirations, offering a more holistic and relational approach to evaluating education's role in advancing soft power objectives.

Multidimensional Engagement

The domain of multidimensional engagement captures the breadth and diversity of relationships formed through education extending across individuals, institutions, and sectors. This aligns with Hong's (2021) category of social capital soft power, which emphasizes the formation of interpersonal networks and institutional linkages that extend a country's influence through sustained educational exchange. The domain also resonates deeply with Knight's (2022) framework of knowledge diplomacy, which reframes international education not merely as a means of influence, but as a collaborative process of strengthening bilateral and multilateral relations across higher education, research, and innovation. Knight (2022) emphasizes the involvement of a wide array of state and non-state actors working in partnerships to address shared challenges. Multidimensional engagement, therefore, reflects the principle of horizontal collaboration across systems, institutions, and levels of governance. To better illustrate how this domain can be evaluated in practice, table 2 outlines representative data collection points aligned with the domain of multidimensional engagement, along with potential interpretation as soft power signals and corresponding placement within the Kirkpatrick model evaluation framework.

Table 2: Multidimensional Engagement data as active engagement across diverse sectors and disciplines to address complex security challenges

Data	Soft Power Signal	Kirkpatrick Level
Participant diversity data (backgrounds, sectors, affiliations)	Broad, voluntary participation reflects credibility and soft power reach	Level 1: Reaction
Stakeholder feedback and co-design input	Co-creation indicates mutual respect and localized influence	Level 1: Reaction
Engagement across perspectives in discussion or collaboration (engagement analytics)	Exposure to diverse viewpoints encourages norm exchange	Level 2: Learning

Long-Term Relationship Building

The domain of long-term relationship building captures the enduring nature of connections formed through educational initiatives that persist beyond the learning experience and evolve into strategic partnerships over time. Hong's (2021) analysis reflected that sustained involvement suggests that the influence of education can extend well past the immediate learning experience, embedding itself in personal, professional, and diplomatic networks. Similarly, Knight's (2022) concept of knowledge diplomacy underscores the importance of durability and reciprocity in partnerships, where long-term benefits accrue to all parties through consistent engagement, joint problem-solving, and mutual respect. Rather than focusing on short-term gains, the domain recognizes that the true value of education in a diplomatic context lies in its capacity to cultivate trust over time, create feedback loops of cooperation, and support institutions and individuals in becoming lasting bridges between nations. Table 3 presents sample data collection points for evaluating long-term relationship building, interpreted through a soft power lens and aligned with Kirkpatrick's evaluation levels. The indicators are intended to capture signs of sustained engagement such as continued collaboration, alumni involvement, and institutional linkages that reflect the deeper strategic value of education as a relationship-based tool for advancing national and regional objectives.

Table 3: Long-Term Relationship Building data as the capacity of the program to cultivate enduring professional and institutional relationships beyond the course or event.

Data	Soft Power Signal	Kirkpatrick Level
Alumni engagement and continued partnerships	Voluntary re-engagement shows affinity and sustained influence	Level 3: Behavior
Joint projects or invitations to collaborate post-program	Diffusion of program values through networked action	Level 3: Behavior
Evidence of network development (e.g., repeat communication, shared outputs)	Ongoing ties point to soft power-based loyalty and cooperation	Level 4: Results

Cultural Humility and Trust

The domain of cultural humility and trust reflects the internal and relational dimensions of cross-cultural learning, those that foster openness, empathy, and mutual respect among diverse actors. This aligns with Hong's (2021) category of cultural soft power, which captures how outbound education programs enhance cultural understanding, language learning, and appreciation of regional customs and values. Knight (2022) emphasizes the importance of mutuality, where partners bring different strengths and gain different, but shared, benefits from the engagement. The cultural humility and trust domain thus highlights that education contributes to international relations not just by increasing attraction, but by building trust through humility, co-learning, and sustained interpersonal understanding. To operationalize the domain, table 4 outlines a few potential relevant data collection points that indicate the presence of cultural humility and trust, the potential interpretation as soft power signals, and alignment with levels of the Kirkpatrick model. The indicators emphasize not only individual learning outcomes but also the quality of relationships and the extent to which participants demonstrate respect, adaptability, and openness to other worldviews.

Table 4: Cultural Humility and Trust data where learners and facilitators approach content and partnerships with openness, self-awareness, and respect for differing worldviews.

Data	Soft Power Signal	Kirkpatrick Level
Reflections or journaling showing growth in self-awareness	Movement toward cultural sensitivity supports trust-building	Level 2: Learning
Partner/community testimonials or interviews	External validation of program's legitimacy and respectfulness	Level 3: Behavior
Inclusive language in materials and facilitation	Program credibility is bolstered through representation and voice	Level 1: Reaction

Norm Diffusion

The domain of norm diffusion refers to the subtle but significant process by which shared values, practices, and standards are transmitted through educational engagement and gradually adopted across cultural and institutional boundaries. Hong (2021) introduces the concept of participatory capital soft power. While difficult to observe directly, it reveals how education can function as a vector for long-term cultural and ideological alignment. Knight's (2022) definition of knowledge diplomacy recognizes the negotiation of values and mutual understanding as essential to meaningful international collaboration. Aligned with Knight's (2022) definition, norm diffusion is not a one-way process of persuasion but a horizontal exchange in which partners co-construct shared principles to address global challenges. As such, the domain focuses on the reciprocal integration of norms, where influence is diffused not through coercion or attraction alone, but through co-learning, institutional adaptation, and mutual benefit. Table 5 outlines representative data points relevant to the domain of norm diffusion, alongside interpretations as soft power signals and corresponding Kirkpatrick levels. These indicators reflect how education fosters not only knowledge acquisition but also alignment with democratic values, legal norms, and cooperative behaviors, all key to understanding how influence is internalized and sustained across cultural and institutional boundaries.

Table 5: Norm Diffusion data as the spread or reinforcement of international norms, legal standards, or democratic values through educational influence

Data	Soft Power Signal	Kirkpatrick Level
Content analysis of learner artifacts showing alignment with shared norms	Adoption without coercion indicates soft power success	Level 3: Behavior
Integration of concepts into policy, training, or institutional practice	Institutional uptake reflects sustained strategic influence	Level 4: Results
Peer/supervisor feedback on observed influence	Confirmation that program learning translated into aligned action	Level 3: Behavior

Emergent Properties

The emergent properties of legitimacy and sustainability represent the highest-order outcomes within the proposed evaluation framework. Because soft power outcomes are not generally directly observable, legitimacy and sustainability are treated as patterns that arise from the interaction of multiple domains (multidimensional engagement, cultural humility and trust, long-term relationship building, and norm diffusion) rather than from any single one. Drawing from systems thinking and contribution analysis, the framework treats these properties as aggregated signals that indicate a program's enduring influence and alignment with soft power objectives. Legitimacy emerges when learners, partners, and institutions perceive the program as credible, contextually relevant, and responsive to mutual needs. This is reflected in voluntary participation, positive stakeholder feedback, and requests for continued collaboration. Sustainability, by contrast, manifests through repeated engagement, post-program partnerships, and institutional adoption of shared values or materials. These properties signal that the influence of education has extended beyond individual learning into sustained, systemic change. Evaluators can identify these emergent outcomes not through isolated surveys or tests, but by tracing consistent patterns across time, roles, and contexts; a mosaic of soft power influence that, while subtle, is both observable and actionable. Evaluating these properties requires interpreting evidence holistically, rather than attributing outcomes to isolated metrics. These are not collected directly but inferred through patterns across domains.

Table 6: Emergent properties of Legitimacy and Sustainability

Emergent Property	Derived From	Indicators
Legitimacy	Multidimensional Engagement + Cultural Humility	High levels of perceived program credibility and relevance Local and partner institutions requesting continued collaboration Voluntary participation from diverse stakeholders
Sustainability	Long-Term Relationships + Norm Diffusion	Repeat engagement or program replication Continued alumni activity after 6+ months Institutionalization of course materials or partnerships

Rubric

Taken together, the domains and associated indicators form the foundation for assessing how education can strategically shape influence over time. When viewed through a systems thinking lens, the domains not only guide data collection but also serve as the basis for interpreting the broader, emergent outcomes of legitimacy and sustainability. To operationalize the approach, the following rubric synthesizes each domain, its representative indicators, and corresponding evaluation levels. The tool is intended to support practitioners and researchers in systematically capturing and analyzing the complex, layered impacts of education as a vehicle for soft power. Table 7 provides a practical tool for evaluators, program designers, and institutional leaders to assess the maturity of educational programs in supporting soft power outcomes. It supports both formative self-assessment and summative evaluation across varying contexts. Importantly, the framework is not intended as a prescriptive checklist, but rather as a flexible diagnostic tool, one that invites adaptation, reflection, and iterative use to support more strategic, context-aware evaluations of educational influence.

Table 7: Rubric

Criteria	Emerging	Developing	Proficient	Advanced
Multidimensional Engagement	Content is siloed and limited to a single domain; minimal cross-disciplinary interaction.	Some integration of different domains; limited opportunities for learner collaboration.	Programs draw from multiple disciplines and include collaborative, real-world problem-solving.	Fully integrated cross-sectoral learning with authentic challenges requiring cooperation across diverse domains.
Long-Term Relationship Building	No sustained interaction beyond the course; minimal alumni tracking or engagement.	Some follow-up mechanisms in place (e.g., newsletters, surveys), but rarely leveraged.	Alumni engagement, peer networks, and post-course collaboration opportunities are supported.	Structured alumni networks, mentorship programs, and ongoing collaboration embedded into the lifecycle of the program.
Norm Diffusion	Norms (e.g., human rights, rule of law) are presented as abstract ideas with no applied learning.	Norms are discussed, but limited to a course module or reading.	Norms are actively explored through applied scenarios and comparative reflection.	Participants actively apply, internalize, and share international norms through scenario-based learning and peer exchange.
Cultural Humility	No attention given to power imbalances, diverse perspectives, or self-reflection.	Some opportunities for discussion of culture or perspective-taking.	Learners reflect on their own assumptions and engage with diverse viewpoints.	Continuous emphasis on reciprocal learning, learner co-construction, and navigating cultural complexity with humility.

Limitations

Some limitations should be acknowledged of the proposed structured framework and rubric for evaluating the strategic impact of education as a tool of soft power. First, the model is conceptual and has not yet been empirically validated across diverse geopolitical contexts. Although grounded in relevant literature and informed by analogous evaluation approaches, its practical utility remains untested in real-world program assessments. Second, the indirect nature of soft power impact makes attribution inherently challenging. The framework relies on contribution analysis and emergent indicators such as legitimacy and sustainability that are subject to interpretation and may vary based on local political, cultural, and institutional conditions. The considerations create a need for careful contextualization when applying the rubric and interpreting results. Third, data collection in the domains of cultural humility, trust, and norm diffusion may depend on long-term tracking, which many education programs are not currently designed to support. Institutional capacity for longitudinal data gathering, alumni engagement, and qualitative analysis may be uneven across organizations. Despite the limitations, the proposed framework provides a valuable foundation for further exploration.

Conclusion and Future Directions

Education has long been recognized as a valuable instrument in international engagement, yet its role as a soft power tool remains underleveraged due to limited frameworks for evaluation and strategic alignment. Robust metrics are essential to determining whether security cooperation efforts, particularly in education, are achieving intended strategic outcomes and delivering meaningful impact. This paper builds on a systems thinking approach to reposition education not as a linear delivery of content, but as a dynamic and adaptive mechanism of strategic influence. By integrating contribution analysis and soft power theory, the proposed model provides both a conceptual foundation and a practical evaluation framework, organized around four interrelated domains: multidimensional engagement, cultural humility and trust, long-term relationship building, and norm diffusion. These domains contribute to the emergent outcomes of legitimacy and sustainability, key indicators of enduring soft power. The inclusion of a rubric and a data interpretation framework offer a structured pathway to assess educational influence beyond traditional learning metrics, while the incorporation of the Kirkpatrick Model aligns short-term learner outcomes with broader strategic effects. Taken together, these tools help shift the conversation from whether education contributes to soft power, to how that contribution can be measured, enhanced, and sustained across complex regional and institutional ecosystems. To amplify education's strategic potential, institutions must evolve their design and delivery practices. This means embedding systems-based methods such as scenario planning, cross-sectoral collaboration, and adaptive learning into curricula that reflect the complexity of contemporary security challenges. Programs should foster inclusive environments that bring together civilian, military, and academic stakeholders to promote mutual understanding and institutional credibility. Moreover, continuity mechanisms such as alumni networks, post-course collaboration, and sustained stakeholder engagement should be integral components of program design to reinforce education as a process of long-term partnership rather than one-time instruction. Finally, the framework invites practitioners and researchers to adopt more rigorous, context-sensitive evaluation practices. Future studies are encouraged to pilot test and refine the rubric in diverse geopolitical and institutional settings. Doing so will enhance its utility not only as a measurement tool but as a flexible diagnostic framework that can inform institutional design, funding priorities, and cross-sector collaboration. The model is not intended as a prescriptive checklist, but as a strategic aid designed to support those seeking to understand, adapt, and amplify the influence of education as a core component of national and international security policy.

References

10 U.S.C. § 342 - Regional Centers for Security Studies. (2017) [https://www.govinfo.gov/app/details/USCODE-2021-title10/USCODE-2021-title10-subtitleA-partI-chap16-subchapV-sec342]

Adhikari, A., & Saha, B. (2023). Projecting soft power: The case of India. Asian J. Educ. Soc. Stud, 38(4), 1–6. https://doi.org/10.9734/AJESS/2023/v38i4829

Admiraal, W., Post, L., Guo, P., Saab, N., Makinen, S., Rainio O., Vuori, J. Bourgeois, J. Kortuem, G & Danford, G. (2019). Students as future workers: Cross-border multidisciplinary learning labs in higher education. International Journal of Technology in Education and Science, 3(2), 85-94.

Akib, A. (2025). Education diplomacy: Understanding global dynamics in interactive and inclusive curriculum design. International Journal of Teaching and Learning, 3(5), 465-475.

Amirbek, A., & Ydyrys, K. (2014). Education and soft power: Analysis as an instrument of foreign policy. Procedia-Social and Behavioral Sciences, 143, 514-516. https://doi.org/10.1016/j.sbspro.2014.07.428.

Antwi-Boateng, O., & Alhashmi, A. (2021). The emergence of the United Arab Emirates as a global soft power: Current strategies and future challenges. Economic and Political Studies, 10(2), 208–227. https://doi.org/10.1080/20954816.2021.1951481

Astleitner, H. (2018). Multidimensional engagement in learning--An integrated instructional design approach. Journal of Instructional Research, 7, 6-32.

Chaban, N. (2024). Collaborative settings of co-creation: Knowledge diplomacy and pedagogical thinking in communication. Journal of Technical Writing and Communication, 54(2), 143-162. https://doi.org/10.1177/00472816231188652

Charles, S. (2023). The role of soft power in international relations. International Journal of Political Science Studies, 1(1), 25-35.

Cull, N. J. (2022). From soft power to reputational security: Rethinking public diplomacy and cultural diplomacy for a dangerous age. In The Routledge handbook of diplomacy and statecraft (pp. 409-419). Routledge.

Desai-Trilokekar, R., & El Masry, H. (2022). The nexus of public diplomacy, soft power, and national security: A comparative study of international education in the US and Canada. Journal of Comparative and International Higher Education, 14(5), 111-133. https://doi.org/10.32674/jcihe.v14i5.4987

El Nsouli, D., Nelson, D., Nsouli, L., Curtis, F., Ahmed, S., McGonagle, I., Kane, R., & Ahmadi, K. (2023). The application of Kirkpatrick's Evaluation Model in the assessment of interprofessional simulation activities involving pharmacy students: A systematic review. American Journal of Pharmaceutical Education, 87(8). https://doi.org/10.1016/j.ajpe.2023.02.003

Foronda, C., Baptiste, D., Reinholdt, M., & Ousman, K. (2016). Cultural humility: A concept analysis. Journal of Transcultural Nursing, 27(3), 210-217. https://doi.org/10.1177/1043659615592

Friman, H., Banner, I., Sitbon, Y., Sahar-Inbar, L., & Shaked, N. (2024). Experiential learning for sustainability: A catalyst for global change. Educ. Adm. Theory Pract, 30, 8508-8514. https://doi.org/10.53555/kuey.v30i5.4404

Gauttam, P., Singh, B., Singh, S., Bika, S., & Tiwari, R. (2024). Education as a soft power resource: A systematic review. Heliyon, 10(1). https://doi.org/10.1016/j.heliyon.2023.e23736

Gelfand, M., Gavrilets, S., & Nunn, N. (2024). Norm dynamics: Interdisciplinary perspectives on social norm emergence, persistence, and change. Annual Review of Psychology, 75(1), 341-378. https://doi.org/10.1146/annurev-psych-033020-013319

Greg, E. (2024). Analysis of three forms of power by Joseph Nye. Advances in Law, Pedagogy, and Multidisciplinary Humanities, 2(2), 162-172.

Habashy, N., & Cruz, L. (2021). Bowing down and standing up: Towards a pedagogy of cultural humility. International Journal of Development Education and Global Learning, 13(1), 16-31. http://dx.doi.org/10.14324/IJDEGL.13.1.02

Hashimoto, S. (2022). Multidisciplinary learning for multifaceted thinking in globalized society. Journal of Systemics Cybernetics and Informatics, 20(6), 43-48. https://doi.org/10.54808/JSCI.20.06.43

Henne, P. (2022). What we talk about when we talk about soft power. International Studies Perspectives, 23(1), 94-111. https://doi.org/10.1093/isp/ekab007

Hong, M. (2021). Evaluating the soft power of outbound student mobility: An analysis of Australia's new Colombo Plan. Higher Education Research & Development, 41(3), 743–758. https://doi.org/10.1080/07294360.2021.1872054

Jalili, D. (2015). The use of professional military education as a soft power asset in US international security policy. Strife Journal, 1, 58-67.

Karadag, H. (2017). Forcing the common good: The significance of public diplomacy in military affairs. Armed Forces & Society, 43(1), 72-91. https://doi.org/10.1177/0095327X16632334

Knight, J. (2022). Understanding and applying the key elements of knowledge diplomacy: The role of international higher education, research and innovation in international relations. In Higher Education Forum (Vol. 19, pp. 1-19). Research Institute for Higher Education, Hiroshima University. 1-2-2 Kagamiyama, Higashi-hiroshima, Hiroshima City, Japan 739-8512.

Lally, M. (2022). Understanding the experiences of Fulbright visiting scholars—A qualitative systematic review. Education Sciences, 12(2), 90. https://doi.org/10.3390/educsci12020090

Larasati, & Asropi. (2025). Training evaluation based on the Kirkpatrick Levels 2 and 3 Evaluation Model: A case study on induction program for novice teachers. Jurnal Borneo Administrator: Media Pengembangan Paradigma Dan Gaya Baru Manajemen Pemerintahan Daerah, 21(1). https://doi.org/10.24258/jba.v21i1.1560

Lipuma, J., & Leon, C. (2024). Trans-disciplinary communication in collaborative co-design for knowledge sharing. https://doi.org/10.22533/at.ed.5584102414032

Lopez, C. T. (2023, April 5). Regional Centers Central to security cooperation, Agency director says. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3352121/regional-centers-central-to-security-cooperation-agency-director-says/

McLauchlin, T., Seymour, L., & Martel, S. (2022). Tracking the rise of United States foreign military training: IMTAD-USA, a new dataset and research agenda. Journal of Peace Research, 59(2), 286-296. https://doi.org/10.1177/00223433211047715

McNerney, M., Sotubo, O., & Egel, D. (2024). Examining the value of a "soft power" net assessment. PRISM, 10(4), 6-23. https://www.jstor.org/stable/48785852

Mishra, N., & Aithal, P. (2023). Modern multidisciplinary education: Challenges and opportunities of modern learning pedagogy. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(4), 270-281. https://ssrn.com/abstract=4745170

Nantulya, P. (2023). Chinese professional military education for Africa: Key influence and strategy. United States Institute of Peace.

Nye, J. (2017). Soft power: the origins and political progress of a concept. Palgrave Communications, 3(1), 1-3. https://doi.or/10.1057/palcomms.2017.8.

Nye, J., 2005. Soft power and higher education. Harvard University, p.14.

Ostashova, Y. (2020, December). Higher education as a soft power tool of state's foreign policy. In Proceedings of the International Conference Digital Age: Traditions, Modernity and Innovations (ICDATMI 2020) (pp. 259-265). Atlantis Press. https://doi.org/10.2991/assehr.k.201212.053

Paul, S., Burman, R., & Singh, R. (2024). Training effectiveness evaluation: Advancing a Kirkpatrick model based composite framework. Evaluation and Program Planning, 107. https://doi.org/10.1016/j.evalprogplan.2024.102494

Saaida, M. B. (2023). The role of soft power in contemporary diplomacy. Journal homepage: www. ijrpr. com ISSN, 2582, 7421. https://doi.org/10.55248/gengpi.4.423.36302

Thomas, I. (2020). Building an impact evaluation toolbox based on an arts and soft power ecosystem. Figueroa Press.

Trunkos, J. (2021). Comparing Russian, Chinese and American soft power use: A new approach. Global Society, 35(3), 395-418. https://doi.org/10.1080/13600826.2020.1848809

Wood, D. (2025). A systems thinking approach to Arctic security education. Journal of Online Graduate Education, 8(1).

Zhu, K., & Yang, R. (2022). Emerging resources of China's soft power: A case study of Cambodian participants from Chinese higher education programs. Higher Education Policy, 36(3), 633–655. https://doi.org/10.1057/s41307-022-00278-w