*Security and Safety*, Vol. 3, 2024010 (2024)
https://doi.org/10.1051/sands/2024010
sands.edpsciences.org

Views OPEN ACCESS

Information Network

# On cultivation of cybersecurity and safety talents and responsible developers

Jiangxing Wu[1,2,3], Hong Zou[1,*], Jiaxi Chen[1], Fan Zhang[3], Yuting Shang[1], and Xinsheng Ji[2,3]

[1] *Fudan University, Shanghai 200433, China*
[2] *Purple Mountain Laboratory, Nanjing 211111, China*
[3] *Digital Switching System Engineering and Technological R&D Center (NDSC), Zhengzhou 450000, China*

Received: 7 February 2024 / Revised: 6 June 2024 / Accepted: 18 July 2024 / Published online: 30 July 2024

**Abstract** To address the serious imbalance between the supply and demand of the cybersecurity workforce, this paper proposes to embrace the latest trend of a fundamental shift in the "underlying dynamics of the digital ecosystem", focusing on a shared liability for cybersecurity between the application side and the manufacturing side. Assuming that product providers shall take more responsibility by implementing secure defaults, this paper explores the establishment of an S&S talent cultivation system to strike the right balance of cybersecurity liabilities by nurturing more responsible developers. This paper proposes a Knowledge, Skill, and Awareness (KSA) model for Security and Safety (S&S) talent cultivation, proves the feasibility of this model by analyzing the theoretical, disciplinary, methodological, practical, and societal foundations of S&S talent cultivation. Additionally, this paper proposes principles and strategies for building a S&S talent cultivation system based on its unique characteristics and patterns. It gives a talent cultivation scheme, supported by an "Independent Knowledge System, Education and Cultivation System, Practice and Training system, Evaluation and Certification system, and Awareness Popularization System". Finally, this paper puts forward a proposal for coordinating efforts and adopting multiple measures to accelerate the cultivation of S&S talents.

**Keywords** Security and safety, Talent cultivation system, Cybersecurity, Endogenous Security and Safety (ESS) theory

**Citation** Wu J, Zou H, Chen J, et al. On cultivation of cybersecurity and safety talents and responsible developers. Security and Safety 2024; **3**: 2024010. https://doi.org/10.1051/sands/2024010

## 1 Introduction

Nowadays, cybersecurity technology is undergoing a paradigm shift [1]. In 2023, the United States unveiled its updated National Cybersecurity Strategy [2], while 18 global cybersecurity agencies collaboratively introduced "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by Design and Default" [3]. Simultaneously, the European Union adopted the Cyber Resilience Act [4], aiming to promote a paradigm shift in the underlying dynamics of the digital ecosystem. In a similar effort to improve manufacturing-side cybersecurity capabilities, this legislation advocates for inherently secure digital products rather than merely more cybersecurity measures. The ultimate goal is to build a "defensible and resilient cyberspace". In response to these developments, there is a growing recognition of the need to transform the cultivation of the cybersecurity workforce. The US underscored this in its 2023 National Cyber Workforce and Education Strategy (as shown in Figure 1), which proposes to "incorporate cybersecurity principles into

* Corresponding author (email: hongzou@fudan.edu.cn)

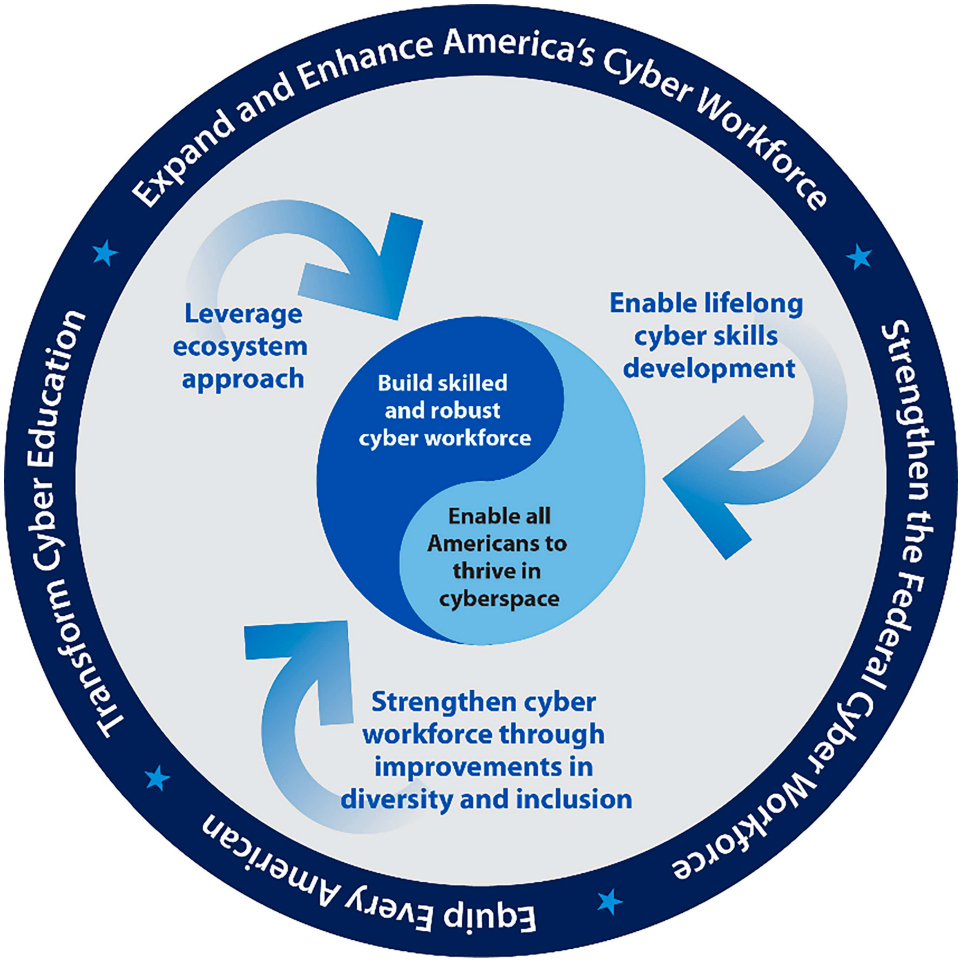


**Figure 1.** Overview of US national cyber workforce and education strategy [5]

engineering work from the earliest to the final stages" and that "participants in the software development process . . . must be equipped to manage the security and privacy implications of the software they create" [5]. By cultivating a cadre of "responsible developers", the aim is to create a collaborative environment where stakeholders across the application side and the manufacturing side work in synergy to fortify cyberspace against threats, as well as to cultivate a cyber workforce comprising both cybersecurity professionals and developers.

The core principle of traditional cybersecurity technology rests on the notion of a distinct segregation between the cybersecurity stage and the design & manufacturing stages of digital products. This model operates by tasking two separate engineering groups to design two distinct systems, with one system being utilized to safeguard the other [6, 7]. Security and Safety (S&S) embodies a fusion of cybersecurity principles within the design and manufacturing phases of technologies and products [8, 9]. This entails the incorporation of cybersecurity features into the design process before development, configuration, and delivery [10, 11], thereby actualizing the concept of "security by design" for digital products [12, 13]. Therefore, the traditional paradigm of cybersecurity talent cultivation, where "developers, defenders, and infiltrators" are relatively isolated, is no longer able to meet present-day demands. Urgent attention is required to embark on research and exploration aimed at nurturing integrated S&S talents. By cultivating a cohort of "responsible developers", we can cultivate a new generation of professionals capable of designing and producing secure-by-default digital products, thus facilitating the paradigm shift in the underlying dynamics of the global digital ecosystem.

Over a decade of exploration and practice, the theory of Endogenous Security and Safety (ESS) has evolved into an Independent Knowledge System with distinctive features. It has provided a scientific foundation for holistically addressing the intertwined challenges of functional safety and cybersecurity. By

amalgamating insights from Information Theory, Cybernetics, Cryptography, Computer Science, and related disciplines, ESS has fostered a methodology system with Systems Theory and Holism as the kernel. China shall unleash its unique advantages as the cradle of ESS theory and technology in cyberspace, cultivate responsible developers equipped with comprehensive knowledge of ESS, adeptness in secure-by-design practices, and a profound understanding of secure-by-default principles. This endeavour seeks to pioneer a new paradigm in the cultivation of S&S talents oriented to essentially resolving the increasingly acute disparity between the supply and demand of cybersecurity professionals. The aim is to align with the notion that "Cybersecurity and informatization are two wings of one body, two wheels of one cart" [14] from the source, while also offering pertinent solutions to the global cybersecurity talent shortage predicament.

## 2 Talent demand and evolving trend

The basic principles for establishing a robust talent cultivation system are demand-based and innovation-driven. In the context of nurturing S&S talents, the priority is to identify the "pain points" and "bottlenecks" impeding talent cultivation in the realm of cybersecurity. By accurately capturing the evolving trends in cybersecurity technology, we can effectively construct a new talent cultivation paradigm that caters to the emerging needs of this field.

### 2.1 The cultivation of cybersecurity talents is facing severe challenges of imbalance between supply and demand

According to the 2023 Global Cybersecurity Outlook [15] released by the World Economic Forum and the latest cybersecurity gap assessment released by the Statista Research Department in January 2024 [16], the global cybersecurity talent gap in 2023 was a total of 4 million, hitting a record high. In China, during the initial establishment of the cybersecurity Discipline in 2012, there was a shortage of approximately 400 000 cybersecurity talents, which expanded to 700 000 in 2017 and further expanded to 1.4 million in 2020. In 2022, an institution released a white paper on cybersecurity talent, stating that there will be a shortage of approximately 3.27 million in China by 2027 [17]. If the growth continues at a rate above, it is predicted that China will face a shortage of around 7 million professionals by 2030. In stark contrast, China currently only cultivates about 30 000 [18] cybersecurity professionals per year, while the annual supply scale of the pan-Informatics workforce does not exceed 1.5 million [19]. In the future, even if all information science graduates from Chinese universities engage in cybersecurity, it's far from enough to fill the industry gap. In the long run, the consequences of this shortage can result in a "black-hole effect".

### 2.2 The lagging development paradigm of the digital ecosystem is the root cause of the talent dilemma

Why is there a serious imbalance between the supply and demand of cybersecurity talents? To shed light on this question, it is required to study the basic model of the cybersecurity talent gap. Here, the analogy of the "doctor-patient model" is used. In the "doctor-patient model", a certain number of residents corresponds to a certain number of medical personnel [20]. Similarly, a certain amount of digital infrastructure corresponds to a certain proportion of cybersecurity personnel, *i.e.*, the number of "bodyguards". However, there is a fundamental difference between the two cases. While the scale of the "doctor-patient model" is estimated according to the Malthusian Population Theory [21], which means that the growth of scale follows a smooth curve, the growth of digital infrastructure follows an index curve. The latter is a non-linear pattern, where the increment far exceeds the stock. To some extent, using the "doctor-patient model" to measure the cybersecurity talent gap can help verify three basic issues. First, the disorderly expansion of digital infrastructure is the root cause of the surge in cybersecurity risks. Secondly, it is impossible to solve the increasingly rampant cybersecurity issues by regarding cybersecurity talents as "bodyguards" and relying on "huge-crowd tactics". Thirdly, without a transformation in the underlying dynamics of the digital ecosystem, the shortage of security governance professionals in digital society cannot be fundamentally addressed. In addition, there are many other reasons for the aggravation of the cybersecurity talent gap. In terms of the education system, the cybersecurity discipline is relatively separated from the electronic information category [22]. In terms of industry needs, manufacturing-side cybersecurity hasn't been given enough attention [23]. In terms of government policy, the regulatory concept is still at the level of "whoever operates is responsible" [24] rather than "whoever manufactures is responsible".

### 2.3 The paradigm shift to the underlying dynamics of the digital ecosystem requires the cultivation of S&S talents and responsible developers

How to fill up the "black hole" in cybersecurity talent? An obvious approach is to make the growth curve of digital infrastructure outside the secure-by-default boundary conform to a smooth curve, with a "Prevention First, Defend Forward [25]" strategy, solving the "snowball effect" of digital infrastructure risks from the source. The "Snowball effect" originates from the fact that digital products themselves have inevitable Endogenous Security and Safety Problems (ESSP), thus the "bodyguard-style" cybersecurity products cannot prove their innocence. Therefore, the triple stack security issues of functional safety, cybersecurity, and even data security of digital infrastructure represent novel types of security threats in the digital society, causing the security risks of the digital ecological environment to be completely out of control, just like a snowball rolling bigger and more severe. So it is urgent to make fundamental changes to the underlying dynamics of the digital ecosystem, and resolutely reverse the imbalance of security liability between the application service side, and the design and manufacturing side. This two-pronged approach can reinforce both supply and demand side security, to provide digital products designed with integrated functional safety and cybersecurity attributes [26–28]. Hence, it's necessary to continue increasing the scale of defenders from the user side, as well as to take unconventional measures on the manufacturing side to cultivate large amounts of "responsible developers" with the concept and ability of "security-by-design". By doing so, we can make digital products, especially digital infrastructure, meet the quality standards of "security-by-default", *i.e.*, being used out-of-box without additional configuration [29, 30].

### 2.4 Cultivating responsible developers becomes a trend in major countries around the world

The United States and Europe have successively introduced "new policies" [31–33] or "new acts" [34–36] regarding cybersecurity. In April 2023, the United States explicitly proposed to "hold developers liable" in its updated National Cybersecurity Strategy. In addition, the United States released the CIE Strategy [37] in 2022 and, National Cyber Workforce and Education Strategy in 2023, proposing a series of talent cultivation initiatives. These initiatives aim to develop digital product developers who possess secure-by-design attributes, and then further reverse the serious imbalance of cybersecurity risks between the "design/manufacturing side" and "user/application side". Although the United States and Europe have begun to promote the cultivation of "responsible developers", there are still three main challenges. Firstly, there is still a lack of fundamental theoretical frameworks and engineering methods to address both cybersecurity and functional safety in an integrated manner, resulting in substituting "process security" for "endogenous security". Secondly, it's difficult to essentially address the inherent inconsistency between functional safety and cybersecurity in the talent cultivation process, resulting in an imbalance like making noodles. If it's thick, add water; if it's thin, add flour. Lastly, developing integrated S&S skills through the cross-fusion of secure-by-design capabilities with existing disciplinary knowledge and competency systems is still operationally challenging.

## 3 Core ideas of talent cultivation

The issue of cultivation objectives is both an old problem and a new challenge, involving theoretical research and reflection, as well as practice and exploration in talent cultivation. Generally speaking, the cultivation objectives provide a basic description of talent cultivation, which plays a regulatory, normative, and guiding role in the cultivation process and is the basic starting point. To effectively cultivate S&S talents, the priority is to delve into the fundamental issue of "what kind of talents to cultivate and how to cultivate them" [38]. The talent cultivation practice shall be premised on an informed understanding of desired objectives, and a scientific and exquisite design of the composition of the Knowledge, Skill, and Awareness (KSA) model [39].

### 3.1 Cultivation objectives of S&S talents

In the cultivation of S&S talents, it is crucial to adhere to demand-based and mission-driven principles. This entails focusing on the evolving needs of the present era, such as the transition towards "leftward" cybersecurity and the simultaneous shift from securing the "application side" to comprehensively securing

both the "application and supply sides". Additionally, it is essential to address the technological requirements arising from the paradigm shift in the digital ecosystem, emphasizing the shift from "external security" to "internal/endogenous security".

The fundamental principle behind S&S talent cultivation is to foster "responsible" developers [40] and develop a new generation of digital technology and industry with ESS attributes. By actively promoting the unique ESS theoretical techniques globally, we aim to stimulate a new round of growth in the global digital industry.

The overall goal of S&S talent cultivation is to nurture a new generation of digital technology professionals with ESS awareness and related knowledge, who possess the design ability and literacy of "security-by-default" and can undertake missions and tasks of responsible developers.

The practical path of S&S talent cultivation is to explore a new paradigm and construct a knowledge genealogy similar to the "reinforced concrete" model to form a matrix and reconfigurable elastic knowledge system with ESS as the framework and multiple security theories supporting each other. It creates a "problem-guided" cultivation mode, with problems as the driving force to create scenarios. It deepens cognition in problem-solving, and learning in practice. It develops an "innovative progress" research field, promotes the ESS school with Chinese characteristics, and jointly builds a safe, reliable, and secure digital future.

### 3.2 Knowledge, Skill, and Awareness (KSA) model of S&S talents

We propose a KSA structure (Knowledge, Explicit Skill × Implicit Skill, Awareness) for S&S talent cultivation [41].

S&S Talents shall possess an ESS knowledge structure. This includes basic theoretical knowledge, basic technical knowledge, design method knowledge, application knowledge, and standard specification knowledge of ESS. By constructing a knowledge structure of ESS, S&S talents can deeply realize the first principle of cybersecurity, profoundly understand the basic method of "Structure determines safety", proficiently master the internal mechanism and application method of "Dynamic Heterogeneous Redundancy" (DHR) architecture implementation, then comprehend the logical relationship between ESS theory and different vertical industry knowledge systems.

S&S Talents shall possess a secure-by-design skill structure. According to the iceberg theory [42], the ability structure is divided into explicit skill and implicit skill. The former refers to the routine application of proficient knowledge and skills, while the latter refers to the ability to solve problems and apply existing knowledge and skills to new scenarios [43]. From the perspective of explicit ability, S&S talents shall have the basic ability to design and implement specific digital systems, including software and hardware design and realization abilities, system architecture ability, system performance testing ability, *etc.* From the perspective of implicit skill, S&S talents shall have stronger ESS ability, that is, the ability to transform and alleviate endogenous security issues in digital systems through structural effect, which is an inherent ability.

S&S Talents shall possess a strong secure-by-default awareness structure. At the core of this awareness is the concept of a responsible developer, someone who upholds secure-by-default quality standards and professional integrity. This awareness becomes ingrained in the consciousness and soul of these talents. The secure-by-default awareness of S&S talents entails prioritizing security in development and design, making "out-of-the-box" security an inherent requirement for the new generation of digital product developers. These developers understand that digital products should not only excel in functionality but also be accountable for the security and safety to their application side.

In order to more clearly illustrate the knowledge skill awareness model of S&S talents, drawing on the US NICE cybersecurity workforce framework [44], this paper gives the CST-KSA framework for S&S talents (as shown in Figure 2). The NICE Cybersecurity Workforce Framework is a mapping model among "Working role-Knowledge, Skill and Ability" (CST mapping) for cybersecurity talents, based on the practices of government, industry, academia, and research constructed by NIST. Referring to the CST mapping method and combining it with Chinese electronics disciplines and specialties, this paper proposes the CST-KSA framework for S&S talents, *i.e.*, the "Knowledge, Skill, and Awareness Model for a new type of talents, oriented to integrated Security and Safety across Manufacturing-Side, Application-Side, and Service-Side". According to this CST-KSA model, the kernel of ESS knowledge base, secure-by-design

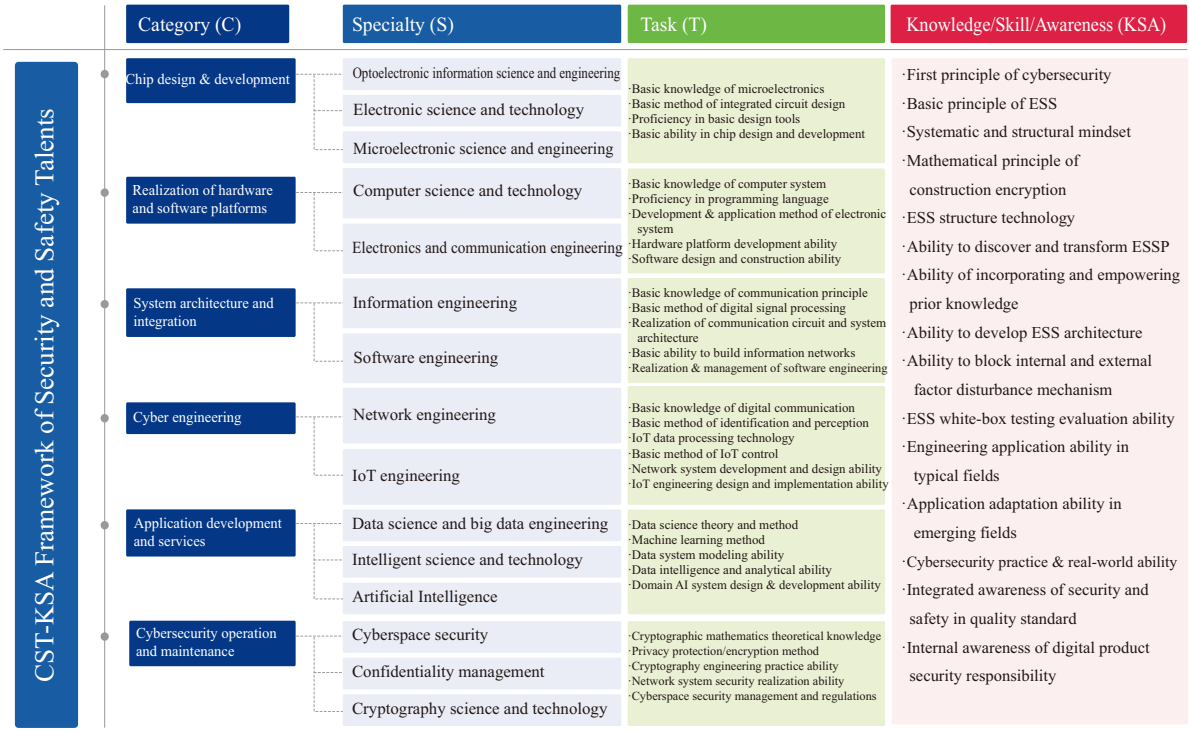


**Figure 2.** CST-KSA framework for S&S talents

skill base, and secure-by-default awareness base are further clarified under different occupational fields and professional categories.

### 3.3 Relationship between Knowledge, Skill, and Awareness of S&S talents

Knowledge, Skill, and Awareness are not separated from each other in our model. On the contrary, the three elements are mutually supportive and converged [45].

ESS knowledge plays a critical role in supporting secure-by-design skill. There is a significant positive correlation between the ESS knowledge system and secure-by-design skills. Specifically, a strong understanding of ESS architecture and system architecture correlates positively with explicit secure-by-design skills. Furthermore, the comprehension of the first principle issue of cyber information systems within ESS is linked to the implicit skill of identifying issues in secure-by-design approaches. Additionally, various theoretical methods that highlight the influence of ESS structure demonstrate a significant positive correlation with the ability to alleviate and transform internal security concerns in secure-by-design practices. This emphasizes the mutually supportive relationship between knowledge and skills in this field.

ESS knowledge needs to be solidified into secure-by-default awareness. There is a significant positive correlation between ESS theory and secure-by-default awareness. The core idea of ESS is "security leftward" [46], "balancing cybersecurity risks and transforming the underlying dynamics of digital ecosystem". It can be vividly said that ESS theory technology can play a subtle role in cultivating "responsible" developers with a "responsible" knowledge system and theoretical framework. "Being responsible" is an integrating point correlating the knowledge structure and awareness structure of S&S talents.

Secure-by-design skill requires secure-by-default awareness as support. There is a significant positive correlation between secure-by-design skill and secure-by-default awareness. Developers lacking secure-by-default awareness struggle not only to cultivate the implicit skills demanded by secure-by-design principles but also to effectively address cybersecurity, functional safety, and data/information security concerns during the architectural design phase. Currently, the biggest cybersecurity problem is that the user side and the manufacturing side mutually pass the buck. Responsible developers, equipped with secure-by-default awareness, consciously shoulder the inherent cybersecurity responsibilities associated with the manufacturing side of digital products.

## 4 Cultivation foundation and feasibility analysis

Exploring the rationale and viability of nurturing S&S talents necessitates a structured framework. Notably, the foundation for cultivating such talents encompasses several key elements, as outlined in documents such as the National Standard on the Teaching Quality of Higher Education Institutions for Undergraduates [47], First-level Disciplines Cultivation Requirements for Doctoral and Master's Degrees [48], among others in China. These foundational aspects include the presence of a robust scientific theoretical base, a well-defined disciplinary base, a methodological base, a practical base, and a societal base. Therefore, to assess the feasibility of cultivating S&S talents, it is imperative to address these five essential dimensions comprehensively.

### 4.1 Scientific theoretical base for cultivating S&S talents

The theoretical basis of Security and Safety can be condensed into the "Security of Security" theory, which scientifically answers several basic theoretical questions regarding the integrated solution of functional safety and cybersecurity [49, 50].

Related studies indicate that the first principle issue of cyberspace threats stems from ESS commonalities. The contradictory nature and related characteristics determine that only evolutionary transformation or reconciliation measures can achieve the goal of unity among opposites, but the contradictory problem itself cannot be eliminated. Given the current stage of technological development and the limitations of human cognitive abilities, it is inevitable that software and hardware will have design vulnerabilities or loopholes that cannot be thoroughly identified or eliminated. The enabling effect of the Von Neumann Computer Architecture [51] and "Stored-Program Control" mechanism [52] to cyberspace makes its "endogenous" security defect a ubiquitous ghost in cyberspace.

The ESS existence theorem proves that if a structure or algorithm has the expression that all three elements of dynamics/randomness (D), variety/heterogeneity (V), and redundancy (R) completely intersect, even in the absence of prior knowledge conditions, any differential mode attacks based on unknown vulnerabilities, backdoors, Trojan virus, *etc.* in a structure, as well as differential mode interference caused by non-human factors such as randomness or uncertainty, can be contained through the endogenous effect of the structure, that is, achieving security goal by separating differential mode security issues from overall security events.

Based on the ESS existence theorem, a structure or algorithm called Dynamic Heterogeneous Redundancy (DHR) for cyberspace with general enabling effects is proposed, which provides a significant theoretical foundation for Security and Safety. DHR structure is a kind of Dissimilar Redundancy Structure (DRS) [53] for functional safety. Through introducing innovative mechanisms such as Dynamic Feedback Control of strategy ruling, Structure Coding, or Environment Encryption, DHR structure embodies many significant features such as "Mimicry Disguises Fog (MDF)", "Entropy non-decrease and Uncertainty Effect", "Generalized Functional Safety Problems Solved by Dimensional Reduction", "Emergent Security Gain (ESG)", and "Structural Encryption (SE)" [49, 50].

DHR can solve engineering technology problems caused by multiple issues such as functional safety, cybersecurity, and even data security in Cyber-Physical Systems (CPS) in an integrated manner, and can enable software and hardware products such as digital systems and control devices with generalized functional safety attributes. In other words, the DHR structure, as a "steel reinforcement" frame of various digital technology products, adopts relevant intrinsic functional technologies and existing or future potential cybersecurity technologies as "concrete" materials to form a CPS system with a "reinforced concrete-like texture", where safety and security can be quantifiably designed and verifiably measured.

### 4.2 Disciplinary base for cultivating S&S talents

The cultivation of S&S talents has a profound disciplinary base and significant interdisciplinary integration characteristics. It involves weaving multiple disciplines together to form a cohesive architecture for addressing Security and Safety (S&S) concerns.

From a philosophical and social science perspective, S&S has rich philosophical implications, "all things are self-contradictory, contradictions are the root of all movements and vitality". According to

materialistic dialectics, the ESS problem (ESSP) is the external manifestation of the interdependence and mutual exclusion among multiple opposite sides within things, it is an inseparable part of things themselves. It can be seen here that the contradiction of ESSP determines that they cannot be fundamentally eliminated, only can be evolved, transformed, or reconciled [54].

From the perspective of Information Theory, according to Shannon's Coding Channel Theory [55, 56], DVR complete intersection can be expanded in time and space as a kind of "Structure Coding" based on the DHR structure or a kind of "Environment Encryption" to counteract the influence of random or nonrandom "Structure Disturbances Noise" (SDN) similar to channel noise.

From the perspective of Cybernetics, it can be recognized from reliability theory that no artificially designed and manufactured physical or logical entity is "perfect". Due to various uncertain factors, functional failure problems can arise at different levels and prerequisites throughout the lifecycle of these entities [57]. When reliability improvement encounters an "uncertain ceiling" problem, the first principle of Cybernetics–Ashyby's Law [58] can be introduced, dealing with the influence of time-varying uncertain factors with the law of Requisite Variety. Wiener's Cybernetics feedback law [59] can be applied to mitigate the negative impact of various uncertain factors through the inhibitory effect of feedback control. Additionally, using the True Relatively Axiom from anthropological sociology [60], a necessary diverse environment can be created to establish a relative identification mechanism that does not rely on prior knowledge. DHR structure, invented based on the above theories, can balance the influence of both human and non-human uncertain disturbance factors according to the "Structural Stability Effect".

From the perspective of Computer, Communication, and Networking, the ESS DHR structure serves as a leading framework for a wide array of technical methods and design principles related to cyber resilience. It functions as a "concrete reinforcement skeleton". ESS-enabled Computer, Communication, and Networking Information technology will effectively respond to various uncertain disturbances introduced by human or non-human factors. This will ensure a reliable executing or operating environment based on the new underlying dynamics of the digital ecosystem, which is urgently needed for sensitive services or applications.

### 4.3 Methodological base for cultivating S&S talents

The traditional security approach is "Reductionism" [61] + "Backward analysis" [62], which essentially follows the mindset of "zeroing out problems". Reductionism involves breaking down cybersecurity issues into smaller, more fundamental components in order to understand and address them effectively. The basic idea of reductionism is to deconstruct a system and meticulously examine the operating principles, vulnerabilities, and weaknesses of its components, to get a profound understanding of its operational mechanism. The research method of reductionism is backward analysis, relying on iterative prior knowledge (library), attempting to discover all security vulnerabilities.

Unlike reductionism, the ESS methodology emphasizes the concept of "Systems Engineering Theory" [63] + "Structure determines safety". It seeks to achieve the engineering objective of global optimization rather than focusing solely on individual or local optimization.

The concept of "Contradiction is the unity of opposites" lies at the core of systems mindset. Similarly, the essence of ESSP lies in the external manifestation of internal contradiction. The primary issue stems from the "Stored-Program Control" mechanism [64], foundational to modern CPS, which fails to differentiate between benign and malicious execution codes, akin to a "gene defect". Even worse, typical problems such as software and hardware design vulnerabilities, have become the most common and challenging generalized functional safety problems in cyberspace. The ESS issues rooted in internal contradictions cannot be eliminated through reductionism. Instead, they can only be solved through the unity of opposites, which requires evolution, transformation, or reconciliation at the system or structural level.

The essence of the Systems Engineering mindset is "Holism" [65]. Guided by the concept of systems theory, the Chinese aerospace community has designed and manufactured world-class system equipment with less advanced components. Their remarkable achievements have proved that "Structure can determine reliability". Similarly, the ESSP of CPSs or digital products neither can be changed by people's subjective will or ideology nor can be completely resolved by supply chain security strategies alone. So do the problems of backdoors and trap doors associated with an "untrustworthy supply chain", which would

not be completely eradicated solely through independent and controllable pathways. The solution lies in establishing a new ESS defence paradigm centred around the concept of "Structure determines safety". Just as Euclidean space triangles have geometric stability, the objective of DHR is to build an algorithm model or structure at the system architecture level that can organically integrate security elements such as dynamics/randomness, variety/heterogeneity, and redundancy, all while expressing gains in terms of integrated Security and Safety.

### 4.4 Practical base for cultivating S&S talents

The traditional objective of cybersecurity talent cultivation focuses on penetration testing, vulnerability discovery, operation, and maintenance. Related training methods include vulnerability analysis and penetration attacks, where individuals are evaluated on their ability to defend against security threats, as well as their skills in vulnerability scanning, penetration testing, code auditing, risk assessment, and security testing. The main goal is to identify and address security risks proactively before malicious attackers can exploit them. To achieve this, cybersecurity professionals employ various techniques to assess the security of a given digital system across different locations, such as internal networks and connection terminals. They aim to discover known vulnerabilities, hidden backdoors, or Trojan viruses that might be present within the system, as well as weak passwords and encryption algorithms with low strength.

Conceivably, future talent cultivation encompasses not only the traditional role of "cyber guardians" on the user side but also a pressing need for cyber resilience engineering technicians on the design and manufacturing side. These professionals are not only proficient in the design skills relevant to their industry but also possess a solid understanding of cybersecurity theories and methodologies. They must have the ability to integrate these two skill sets and apply them effectively to the development of products or digital systems in their respective fields or industries. This holistic approach ensures that cybersecurity considerations are ingrained into the very foundation of the design and manufacturing processes, bolstering the overall resilience of the systems being developed.

Following the gold standard of verification established by the ESS theory–"white-box injection" test, we recommend a unique "white-box" test method [66] to provide a practical training environment for the cultivation of S&S talents. This method allows for the measurement, verification, and explicit expression of the competency of the trainees. It enables trainees to learn the principles of how ESS structure transforms various test disturbances into simple properties of either differential or common mode events within the DVR domain, even in the absence of comprehensive prior knowledge and real-time conditions. Moreover, the method enables trainees to understand the systematic response to these events, which may include the automatic elimination or bypassing of injected test examples via scheduling, configuration, or reconstruction of the software or hardware environment. It provides hands-on experience to observe how resilient recovery from inductive, common-mode escape events is achieved and whether the tested operational environment can recover from non-inductive escape events within a specified time frame. Through this immersive experience, the significance of "white-box injection" is clear to trainees as the "gold standard" of detecting the presence of an ESS structure effect within a system. Trainees will understand that even if there are vulnerabilities and backdoors in the control loop, it is difficult for malicious actors to exploit them through surface attacks.

### 4.5 Societal base for cultivating S&S talents

China is the birthplace of ESS theory and technology. After nearly a decade of efforts, China has formed a broad consensus in promoting the development of ESS design technology and the transformation of the cybersecurity responsibility to the manufacturing side. At the 2023 Wuzhen Summit, the concept of "Creating an Inclusive and Resilient Digital World Beneficial to All – Building a Community with a Shared Future in Cyberspace" [67] was proposed. The term "resilience" first appeared at the Wuzhen Summit, demonstrating the Chinese government's basic attitude towards the development of the digital world. Security is an important prerequisite for resilience, without secure and reasonable cyberspace governance, it will be difficult to sustain the development of the digital world. Meanwhile, many Chinese experts and scholars also call for accelerating the related work. "Establishing a robust cybersecurity assurance framework is vital for a resilient digital landscape, yet the path forward

remains arduous" [68]. The pursuit should encompass 5 elements including supply chains, technology systems, upcoming challenges, infrastructure, and talent development. In October 2023, several prominent Chinese universities–Fudan University, Zhejiang University, University of Science and Technology of China, and Southeast University–issued the "Xinghua Consensus" and proposed to build a partner relationship. This consensus and partnership aims to foster responsible developers to balance cybersecurity risks and achieve a digital ecological shift [69]. China's front-runners in cybersecurity and information technology are showing a keen focus on pioneering cybersecurity technologies and the nurturing of skilled professionals. They advocate for "integrating security as a core part of new digital infrastructures" [70], and for affirming "cybersecurity as the crucial backbone for the growth of the digital economy, must embed cybersecurity capabilities throughout the development of digital cyberspace" [71].

The growing social emphasis on cybersecurity responsibility within the manufacturing sector is providing buoyant employment prospects for S&S talents and responsible developers. This begins with the innate interdisciplinary advantage which serves to bridge the gap between current educational frameworks and the needs of the market, fostering creative and adaptable expertise. Secondly, S&S talents possess a natural trait of innovation. The heightened focus will be placed on nurturing problem-solving thinking and technical innovation in students, opening doors to more entrepreneurial opportunities and access to resources. Furthermore, the intrinsic capacity for continuous learning and skill renewal, particularly the application of ESS theory across varied fields and scenarios, will equip individuals to thrive in an ever-evolving professional landscape. Additionally, the natural propensity to transcend industry boundaries and engage in collaborative innovation, inevitably will further cross-disciplinary and inter-industrial dialogue, and enrich the pool of innovative thoughts and progress. It can be seen that cultivating S&S talents and responsible developers is poised to instigate a paradigm shift in the cultivation of digital infrastructure talents.

ESS theory, as the theoretical kernel of S&S talent cultivation, has formed a systematic, complete theoretical and technical system through continuous improvement and practical exploration since it was proposed in 2008. It has underpinned the publishment of several monographs such as ⟨An Introduction to Cyberspace Mimic Defense⟩ [49], ⟨Cyberspace Endogenous Security and Safety: Mimic Defense and Generalized Robust Control⟩ [50], ⟨Endogenous Security and Safety empowers Cyber Resilient Engineering⟩ [72], applying for over 200 international/domestic patents. Since 2018, the "Qiangwang" International Elite Challenge on Cyber Mimic Defense has been held for six consecutive sessions, with hundreds of domestic and overseas hacker teams competing. It has provided a platform for cybersecurity talents' practical training for more than ten colleges and universities. Since 2017, Nanjing Purple Mountain Laboratory (PML) has built the "Network Endogenous Security Testbed" (NEST), which provides a common platform for domestic and overseas colleges and universities to cultivate practical ESS and secure-by-design talents. It promotes the practical exploration of S&S talent cultivation. Meanwhile, it's crucial to acknowledge that the cultivation of S&S talent remains primarily theoretical and is founded on limited teaching practices. Further exploration is required to integrate it into academic qualification education and align it with talent cultivation systems rooted in disciplinary specialities.

## 5 Cultivation system and practical path scheme

### 5.1 Building strategy of Security and Safety (S&S) talent cultivation system

Cultivating S&S talents requires paradigm innovation, which shall start from understanding the theoretical and methodological underpinnings of Security and Safety.

*The competency-based perspective.* This shift calls for a pivot from the traditional "knowledge-based" [73] education system to a "competency-based" [74] approach, where the core focus is on cultivating the ability to identify and address real-world problems. The ESS theory arose from problems, hence, the education of professionals in these areas should also be problem-centric, connecting the education context with societal needs. This is different from the outdated method of distributing "static knowledge" like frozen goods in the fridge to students. Rather, we need an approach that emphasizes "experiential learning in a specific context" [75], encouraging students to gain knowledge and improve competency through solving real-world problems. This approach not only imbues them with knowledge but also hones their skills and personal development, equipping them to solve practical challenges effectively.

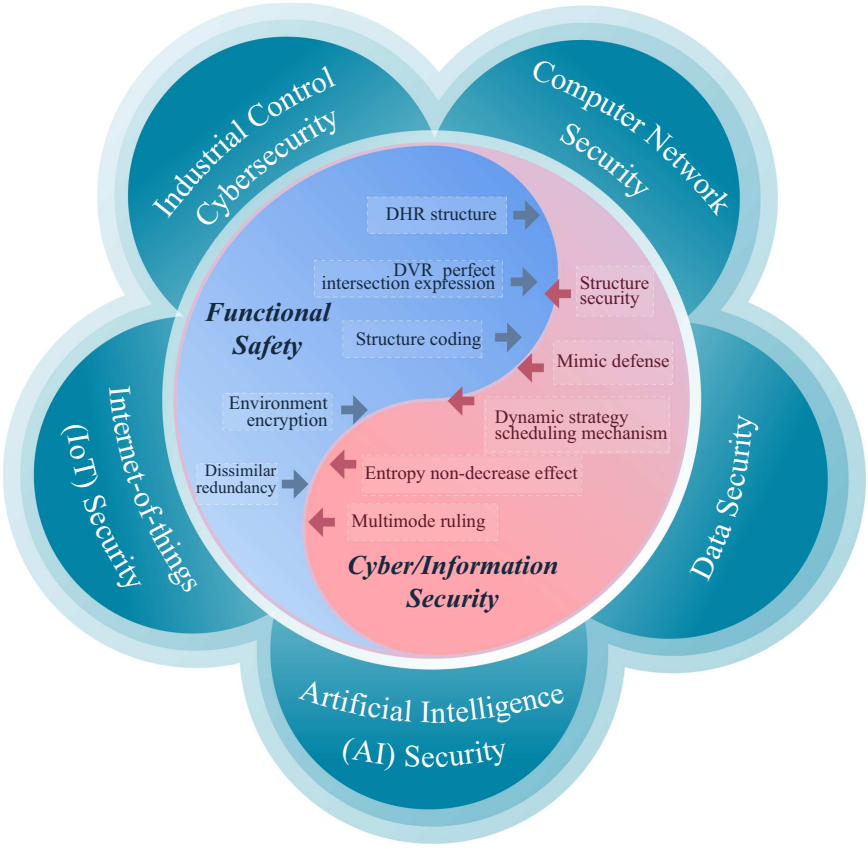


**Figure 3.** S&S Knowledge Bedrock based on the convergence of ESS theory

*The intrinsic motivationoriented principle* [76]. According to Dewey's Empirical Learning Theory, learners don't simply store external information in memory; instead, they gain a surge of knowledge from their experiences and empirical interaction with the external world [77]. In the cultivation of S&S talents, it is necessary to stimulate students' innate capacity for self-directed learning, transitioning from reliance on an "external drive" to an "internal drive" [78]. Educators must guide students to construct their frameworks of knowledge, deepening their grasp of cybersecurity's core principles and the intrinsic challenges of maintaining security. This process entails a fluency in the concept that "Structure determines safety", understanding the interplay between system architecture and security mechanisms. Moreover, students should be encouraged to develop integrated thinking for comprehensive solutions that encompass both functional safety and cybersecurity. This method will prepare them with both the depth and flexibility needed to meet the complex demands of today's safety and security challenges.

*The learningbydoing principle* [79]. Given that the ESS theory is grounded in practical and engineering applications, proficiency in secure-by-design methodologies must be honed through hands-on engineering experiences. The journey to develop S&S expertise is, in a sense, one of unearthing, evaluating, learning, and resolving problems. During this cultivation process, it is vital to summarize and extract emerging issues across new domains induced by the trend that functional safety, cybersecurity, and information/data security are interwoven together. It involves fostering practical skills by fully leveraging knowledge, competences, and properties to creatively solve problems. By centering the educational experience on problem-solving and continuous innovation, the quality of talent development will be significantly enhanced, equipping professionals with real-world proficiency.

*The "reinforced concrete" effect.* The ESS structure serves as a robust "reinforced concrete" backbone. Its intrinsic fusion mechanism can as seamlessly assimilate various traditional cybersecurity technologies as "concrete materials" can bond aggregate together to harden into a rigid mass (as shown in Figure 3). Crucially, the ESS theory is expected to reconcile the longstanding "two skins" discrepancy between the knowledge systems of functional safety and cybersecurity. By leveraging the "reinforced concrete effect", it can harmonize a diverse range of technologies and knowledge from traditional IT, ICT, IoT

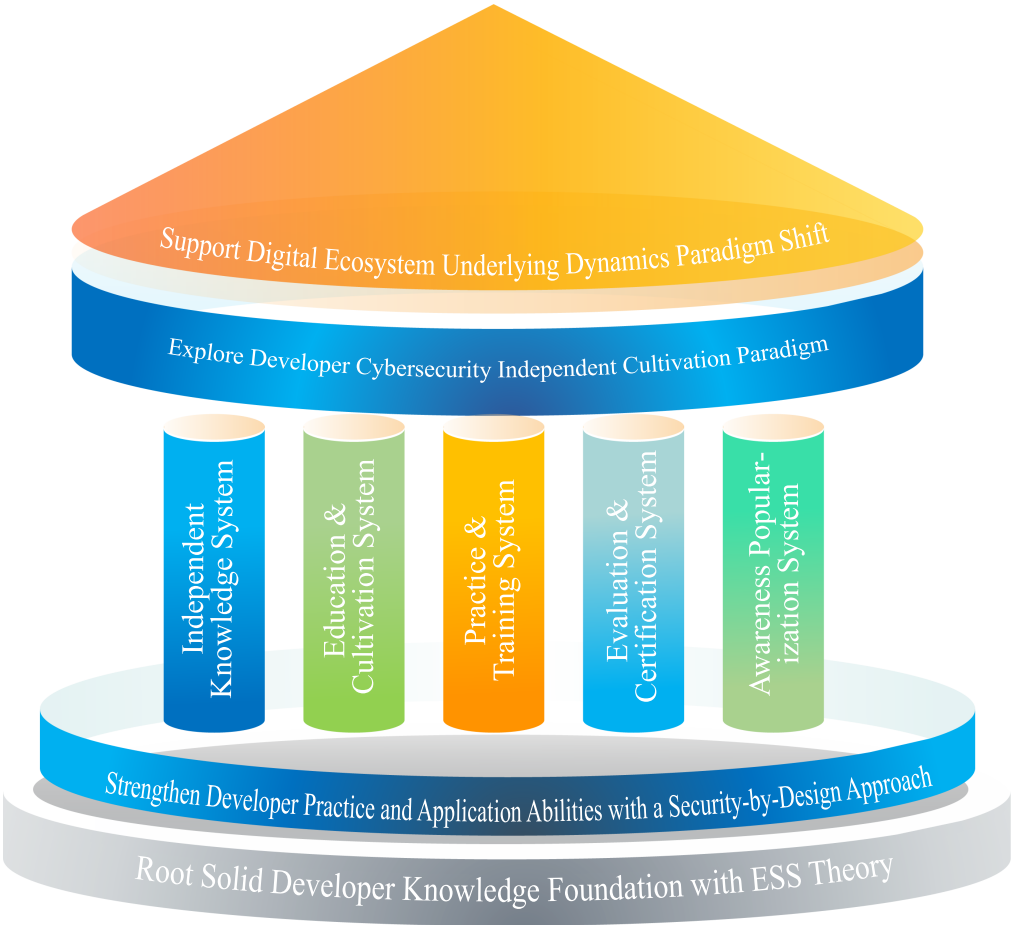


**Figure 4.** Cultivation architecture design of S&S talent called "Five-Colored-Stone Scheme"

sectors, cybersecurity frameworks, and open-source communities. This convergence and fusion lay a solid foundation of knowledge for S&S expertise.

### 5.2 Architecture design of the cultivation system

The architecture design of the cultivation system of S&S talents includes Independent Knowledge System, Education and Cultivation System, Practice and Training System, Evaluation and Certification System, and Awareness Popularization System and is called "Five-Colored-Stone Scheme", as shown in Figure 4.

*Independent Knowledge System.* The foundation of any successful talent cultivation lies in a robust knowledge system. The creation of S&S experts with an ESS knowledge base calls for the establishment of an ESS Independent Knowledge System. Over nearly a decade, the ESS theory has undergone continuous refinement to emerge as a distinct school of thought in the cybersecurity realm. Characterized by logical coherence and theoretical consistency, it has explored innovative methods for cyber resilience rooted in the premise that structure dictates security. It has brought up a new concept of holistic Security and Safety, laying the groundwork for the development of a Chinese Independent Knowledge System dedicated to cybersecurity. The structure of the ESS Knowledge System can be envisioned as a tree composed of roots, branches, and leaves (as shown in Figure 5). The "Root" comprises all foundational ESS theories and technologies. The "Branch" technology extends to interdisciplinary applications across various fields and industries that ESS enables. Meanwhile, the "Leaf" technology encapsulates the specific implementation techniques of ESS and its dynamically evolving technological expressions. As an autonomous and leading system, the unique and original ESS Knowledge System possesses outstanding integrative power and cohesiveness, ensuring its relevance and efficacy in the evolving landscape of cybersecurity.

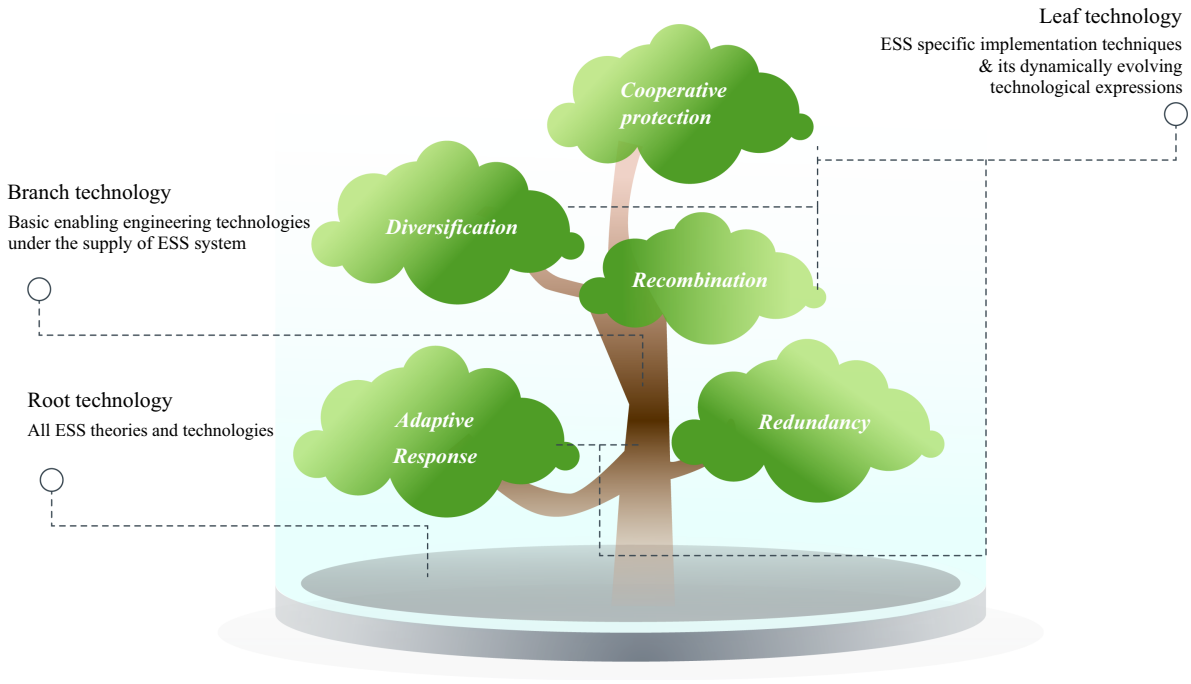


**Figure 5.** Tree of ESS knowledge system

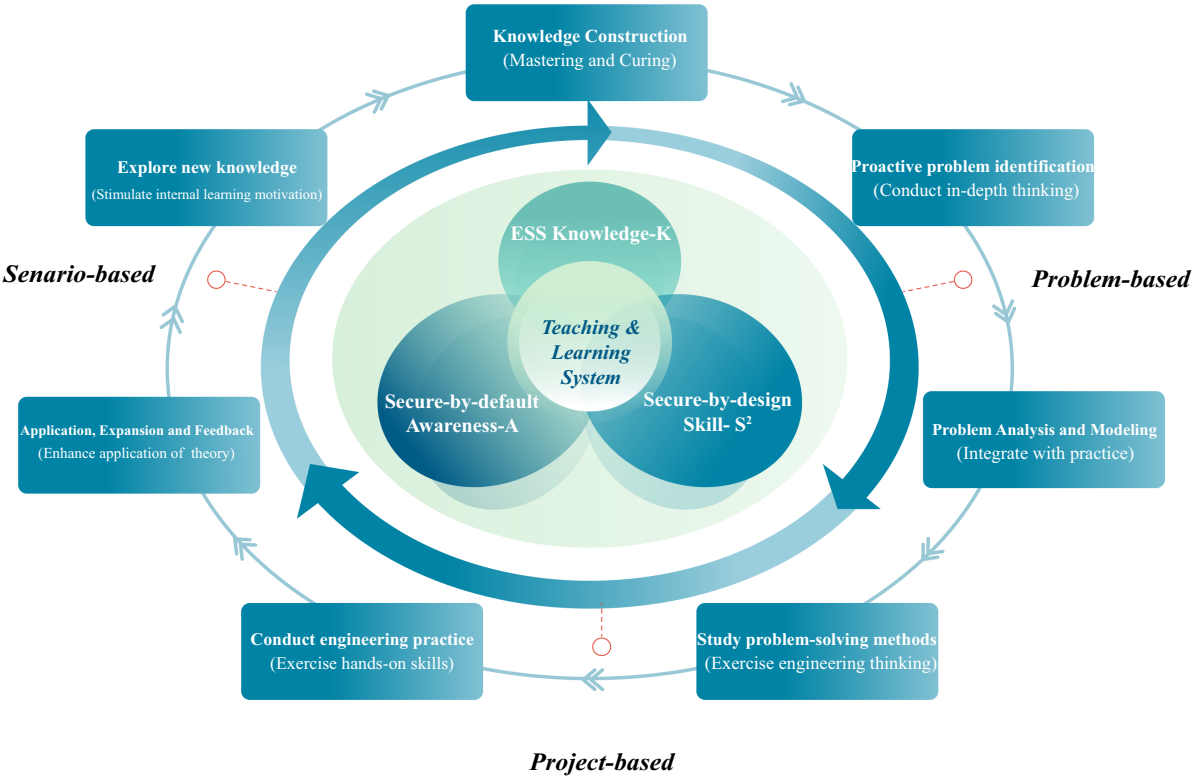


**Figure 6.** Teaching & Learning session design for S&S talents

*Education and Cultivation System.* The Education and Cultivation System plays a pivotal role in shaping S&S professionals who are well-rounded, embodying the trifecta of knowledge, skilful competence, and quality in both functional safety and cybersecurity [80]. This necessitates a departure from

traditional education models that focus primarily on curriculum, textbooks, and instructors [81]. Instead, the approach should pivot towards a dynamic, skill-oriented pedagogy that incorporates the "reinforced concrete" effect of the knowledge system to solidify students' S&S competencies. This system should prioritize mission-driven guidance and the nurturing of responsibility, encouraging uniqueness and innovation. It must bolster self-directed learning initiatives and foster internal motivation [82], empowering students to take charge of their educational journeys. Additionally, problem-oriented guidance and situational learning are key strategies [83] that dictate "learning by doing" [84] or "experiential learning" [85] (as shown in Figure 6). The talent cultivation pattern envisioned here is one characterized by collaborative education [86], where students and teachers work in tandem, and where cross-disciplinary, inter-institutional, and industry-academic alliances drive the education process.

*Practice and Training System.* To practice advanced educational principles such as "learning by doing", "problem-oriented teaching" [87], "contextual teaching" [88], and "collaborative education" [89], it is imperative to establish an innovative Practice and Training System [90]. This requires fully utilizing the capabilities of the ESS testing environment to address challenges associated with developing practical platforms and setting hands-on training modules. Leveraging facilities like Purple Mountain Laboratories' NEST2.0 can provide a standardized training arena [91] for nurturing S&S talents and responsible developers, addressing the pressing need for systematic training in secure-by-design practices. Additionally, the implementation of virtual teaching and research classroom models [92, 93] can alleviate the scarcity of instructors for practical training sessions, facilitating the formation of a new structure for pedagogic research and community-based organizational strategies that underscore co-creation and the sharing of educational resources. Competitions such as the Prosperous Qiangwang International Elite Challenge On Cyber Mimic Defense [94] revolutionize the "white-box" based human-machine interaction into a competitive showcase of practical skills between "product developers" and "cybersecurity attackers/defenders". This platform not only allows a greater number of students to demonstrate their capabilities and ingenuity but also serves as a testament to their potential value in the cybersecurity arena.

*Evaluation and Certification System.* The Evaluation and Certification System serves as a crucial bridge for S&S professionals in their transition into the workforce, embodying the "last mile" of their educational journey. The pressing challenge here lies in harmonizing the supply from the education domain with the demand of society and industry [95]. Drawing on educational best practices, the establishment of a certification model for these professionals is pivotal. Enhancing the credibility and appeal of this model will broaden the qualification pathways available to responsible developers. To build a practical, project-based certificate assessment and evaluation structure, leveraging resources like Crowd-sourced Testing platforms and the NEST facility's accumulated practical educational assets is essential. This aligns with the "credit bank" system [96], which rewards developers for solving real-world problems on authentic platforms. Such a system not only bolsters the alignment between problem-solving and certificate education but also incentivizes ongoing learning and skill development. Furthermore, the prestige and trustworthiness of certificate education must be cultivated, considering the recognition from industry and enterprise as the driving force. Employer satisfaction should be the cornerstone of training objectives. The success or failure of training should not be self-evident but should go back to the source of the demand for talent training, and be commented on by the industry and enterprises [97]. It's necessary to have quantifiable and explicit criteria for certification and evaluation. To facilitate practice, this paper, based on the CST-KSA model, constructs a "three-dimensional certification and evaluation standard model for S&S talents" (as shown in Figure 7).

*Awareness Popularization System.* The cultivation of S&S talents demands society-wide engagement, underscoring the need for widespread education on ESS theory and technology to foster a comprehensive understanding and global collaboration, nurturing a burgeoning ESS ecosystem. On one front, it's essential to embed a security consciousness throughout the entire lifecycle of the digital ecosystem. This core ideology should weave through all phases of software and hardware development and their operational processes, from requirement analysis and conceptual design to deepening design, followed by development, testing, verification, large-scale deployment, then operation and maintenance (as shown in Figure 8). Concurrently, it's crucial for social pillars–universities, research institutes, leading corporations, and popularized science organizations–to collaborate in demystifying the first principle in cybersecurity and the ESS contradictions (as shown in Figure 9). This collective effort aims to enlighten the public on the potential of the new ESS paradigm, reinforcing trust in theories and methodologies capable of mitigating "unknown unknown" security threats, even in the absence of prior knowledge. In unpredictable

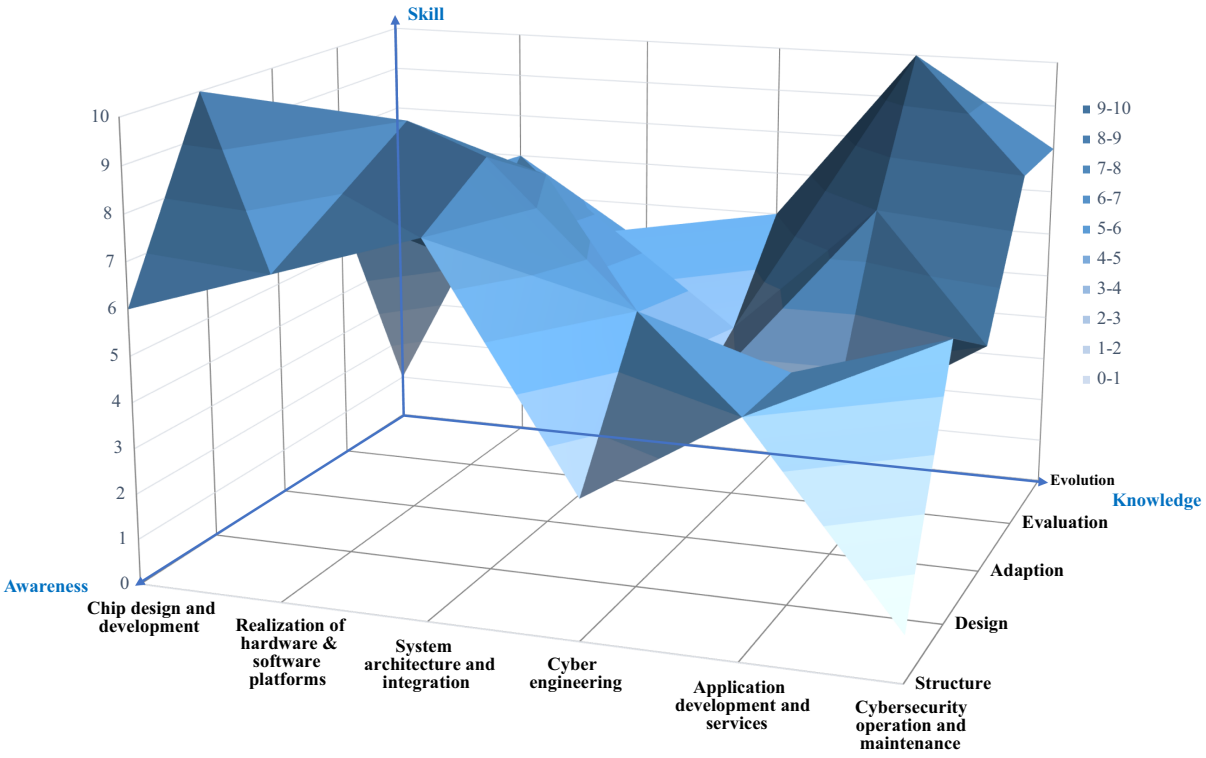


**Figure 7.** 3D certification and evaluation standard model for S&S talents

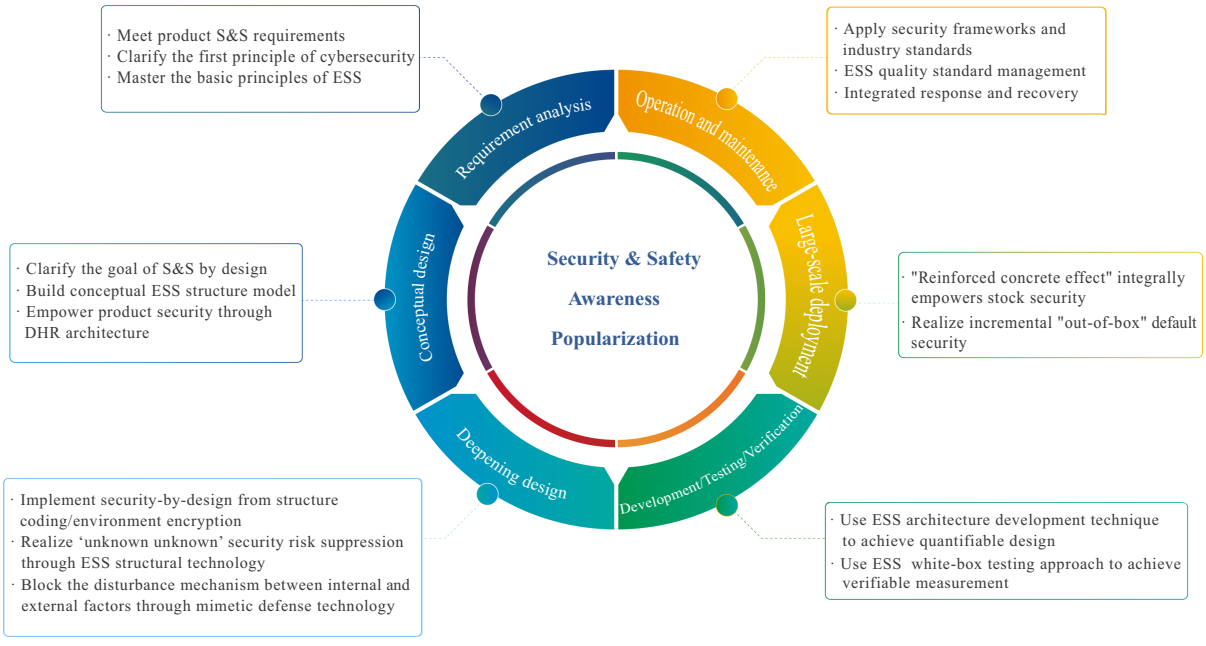


**Figure 8.** S&S awareness architecture process and promotion system design

cyberspace, where "credibility can't be assured or genetic flaws are present", we can still address multifaceted issues like functional safety, cybersecurity, and data/information security in a holistic manner through "Structure Coding/Environment Encryption".


**Figure 9.** Design concept for ESS theory scientific popularization system

### 5.3 Related suggestions for accelerating the building of the S&S talent cultivation system

From the government's standpoint, it is imperative to enhance legislation in the field of cyber resilience by drawing on the legislative expertise of developed countries. This will enable the imposition of legal restraints on the norms across the entire digital product process, with a particular focus on the cybersecurity obligations of digital product designers, developers, and manufacturers. It will foster a stringent demand for S&S specialists.

In the realm of education, there is a pressing need to redouble efforts to foster the growth and advancement of the ESS Independent Knowledge System with distinctive Chinese characteristics. By rooting ourselves in the context of Chinese unique circumstances and prioritizing the resolution of critical bottlenecks, we can establish an independent, cutting-edge knowledge system that not only benefits China but also enriches the global scholarly landscape. This system will provide robust support for the cultivation of well-rounded S&S professionals.

From an industry standpoint, it is crucial to proactively advance the S&S certificate education system. This endeavor aims to aid developers of digital products and critical information infrastructure systems in particular to successfully meet the requirements of S&S competency assessments. The ultimate objective is to make S&S awareness, theoretical knowledge, and methodology an essential component of the education curriculum for every designer and developer. In addition to enhancing the skills of existing professionals, there is a further need to prioritize leadership in nurturing emerging talents. By leveraging diverse and modular certificate education platforms, we can equip future digital product developers with secure-by-design capabilities and secure-by-default consciousness. This will ensure that their products meet "out-of-box cyber resilience" standards.

From a social perspective, it's essential to promote widespread collective awareness of security, safety, and quality requirements for digital technology products. Product manufacturers need to bear the responsibility for the quality of digital security products, while society as a whole must recognize that manufacturers hold the "primary responsibility" for cybersecurity as well. It should be mandatory for all digital products to meet cybersecurity quality standards before entering the market. "Out-of-box" and "Security-by-default" are becoming a Must option for society, rather than merely an optional technical feature to enhance the product's appeal. Through building social consensus, the manufacturing sector is compelled to develop a strong sense of responsibility and fulfil its cybersecurity obligations towards consumers and the digital society.

## 6 Summary and outlook

In conclusion, the cultivation of S&S talents can be summarized as follows:

The motivation for cultivating S&S talents stems from the global shift in the underlying dynamics of the digital ecosystem. The goal is to foster the development of professionals on the design and manufacturing side who possess a strong foundation of ESS knowledge, secure-by-design skills (both explicit and implicit), and a secure-by-default mindset tailored to specific domains or industries. From the perspective of policymakers, the key to driving the transition is adjusting the governance philosophy of cybersecurity, *i.e.*, a shift from "whoever operates is responsible" to a sharper focus on "whoever manufactures is responsible".

This cultivation is built upon an ESS Independent Knowledge System, characterized by its intersectional theoretical foundations, interdisciplinary foundations, methodological framework, and practical guidelines. It continuously evolves and matures while embracing scientific principles and inclusivity. Meanwhile, as far as talent cultivation is concerned, more attention should be paid to technology ethics [98], focusing on the knowledge and theories of privacy protection, technology for the good, and the equal importance of security and development.

The mode of cultivating S&S talents is determined by its internal thinking model. The ESS theory emerges from deep reflection and paradigm innovation regarding ESS issues. Consequently, the cultivation of S&S talents inherently adopts a kind of "problem-driven + context-based + collaborative + self-driven" learning approach [99]. In fact, more emphasis should be placed on the improvement of practical skills and empirical capabilities for S&S talents [100]. It is essential to strengthen the construction of hands-on training environments and real-world scenarios, and to establish a training mode of "learning by doing" and "combining hands-on and brains-on". These will ensure that talent cultivation is more sustainable and able to continuously adapt to technological and societal trends.

In the cultivation of S&S talents, it is essential to foster and establish a social consensus. The public must develop a deeper understanding of what cybersecurity responsibilities the manufacturers should bear, and reject the constant unfair "passing bucks", *i.e.*, passing unlimited cybersecurity responsibilities and costs to users. This consensus will facilitate the development of a robust talent cultivation system focused on Security and Safety. On a broader scale, the development of S&S talents requires extensive international cooperation [101]. Currently, there exists a widespread international consensus on a paradigm shift in the underlying dynamics of the digital ecosystem. This consensus provides a solid footing for enhancing international cooperation in bolstering the cultivation of S&S talents.

S&S talents have a vast career market, natural interdisciplinary advantages, innovative traits, and the inherent ability to continuously learn and update skills. All these factors will serve as drivers and exemplars for the cultivation of "New Engineering" talents [102].

#### Conflict of interest

The authors declare no conflict of interest.

#### Data Availability

No data are associated with this article.

#### Authors' Contributions

Jiangxing Wu laid the theoretical and ideological foundations of this paper, providing strategic guidance on S&S talent cultivation. Hong Zou designed the whole frame and structure of the paper. Jiaxi Chen designed the CST-KSA S&S framework and evaluation 3D model. Fan Zhang mainly surveyed the existing cybersecurity talent/workforce theories and updates. Yuting Shang improved the readability of the paper by grammatical modification and polishing. Xinsheng Ji provided important thoughtful and practical guidance from the experimental perspectives.

#### Acknowledgements

Thanks to Nenghai Yu, Yufeng Li, Kui Ren and other experts for their experience shared about cybersecurity talent cultivation in the Xinghua Meeting; thanks to Jinhu Jiang, and Fengzhe Zhang for their helpful suggestions and comments on the ESS talent framework; thanks to anonymous reviewers for their hard work and kind help.

#### Funding

This work was supported by the Chinese Academy of Engineering Strategic Research and Consulting Program (No. 2023-XZ-11).

## References

[1] Wu J. Development paradigms of cyberspace endogenous security and safety. Sci China Inf Sci 2022; **65**: 156301.
[2] US National Cybersecurity Strategy. Washington: The White House, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[3] CISA, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default, 2023, https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
[4] European Commission. The European Cyber Resilience Act (CRA), 2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[5] Office of the National Cyber Director. National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf
[6] Brewer DFC. Applying security techniques to achieving safety. In: Redmill F and Anderson T, editors, Directions in Safety-critical Systems, Springer, London, 1993, 246–256.
[7] Leveson NG. Safeware: System Safety and Computers. New York, NY, USA: ACM, 1995.
[8] Kriaa S, et al. A survey of approaches combining safety and security for industrial control systems. Reliab Eng Syst Safety 2015; **139**: 156–178.
[9] Hunter B. Integrating safety and security into the system lifecycle. In: Improving Systems and Software Engineering Conference (ISSEC), Canberra, Australia, 2009, 147.
[10] Kornecki AJ and Zalewski J. Safety and security in industrial control. In: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, New York, NY, USA, 2010, 1–77.
[11] Johnson CW. CyberSafety: On the interactions between CyberSecurity and the software engineering of safety-critical systems. In: Dale C and Anderson T, editors, Achieving System Safety, Springer-Verlag, London, UK, 2012, 85–96.
[12] Cavoukian A and Chanliau MD. Privacy and Security by Design: An Enterprise, Architecture Approach. Ontario: Information and Privacy Commissioner, 2013.
[13] Katina PF and Keating CB. Cyber-physical systems governance: A framework for (Meta)cybersecurity design. In: Masys A, editor, Security by Design. Advanced Sciences and Technologies for Security Applications, Springer, Cham, 2018.
[14] Wang S. On information security, network security and cyberspace security. J Lib Sci China 2015; **41**: 72–84.
[15] World Economic Forum, Global Cybersecurity Outlook 2023, https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf
[16] Statista Research Department. Cybersecurity Gap Assessment Worldwide 2023, by Country, 2024, available at: https://www.statista.com/statistics/1275691/cybersecurity-jobs-gap-by-country/
[17] Cybersecurity Talent Practical Capabilities White Paper Released, China Information Security 2022, 100.
[18] Cybersecurity Research Institute of China Academy of Cyberspace, Building a Strong National Cybersecurity Barrier – Achievements and Changes in the Development of China's Cybersecurity Work, China Network Information, 2022.
[19] Number of Regular Students for Normal Courses/Short-cycle Courses in HEIs by Discipline in 2022, Ministry of Education of the People's Republic of China, http://www.moe.gov.cn/jyb_sjzl/moe_560/2022/quanguo/202401/t20240110_1099511.html
[20] The National Health Workforce Accounts database, World Health Organization, Geneva (https://apps.who.int/nhwaportal, https://www.who.int/activities/improving-health-workforce-data-and-evidence)
[21] Malthus TR. An Essay on the Principle of Population, as it Affects the Future Improvement of Society. With Remarks on the Speculations of Mr. Godwin, M. Condorcet, and Other Writers. Harmondsworth: Penguin, 1970.
[22] Ramirez RB. Making Cyber Security Interdisciplinary: Recommendations for a Novel Curriculum and Terminology Harmonization. Cambridge: Massachusetts Institute of Technology, 2017.
[23] Bajaj M and Akhilesh KB. Understanding the need for cybersecurity in manufacturing environment. In: Akhilesh K and Möller D, editors, Smart Technologies, Springer, Singapore, 2020.
[24] Li W. Ecosystem thinking and institutional frameworks for cybersecurity governance in digital organizations. Frontiers 2024: 93–101.
[25] Corn GP and Emily G. Defend forward and persistent engagement. In: Goldsmith J, editor, The United States Defend Forward Cyber Strategy: A Comprehensive Legal Assessment, Oxford Academic, New York, 2022.
[26] Piètre-Cambacédès L and Bouissou M. Cross-fertilization between safety and security engineering. Reliab Eng Syst Saf 2013; **110**: 110–126.
[27] Ellis A. Integrating Industrial Control System (ICS) safety and security–A potential approach. In: Proceedings of the 10th IET System Safety and Cyber-Security Conference 2015. IEEE Xplore Digital Library 2015, 1–7.
[28] Riel A, et al. Integrated design for tackling safety and security challenges of smart products and digital manufacturing. CIRP Ann 2017; **66**: 177–180.
[29] Cybersecurity and Infrastructure Security Agency CISA, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software, 2023, available at: https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf
[30] Von Solms S and Futcher LA. Adaption of a secure software development methodology for secure engineering design. IEEE Access 2020; **8**: 125630–125637.
[31] NIST. Developing Cyber-resilient Systems: A Systems Security Engineering Approach: NIST publishes SP 800-160 vol. 2, Revision 1, 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf
[32] NIST, US Department of Commerce, Secure Software Development Framework, 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf
[33] Federal Communications Commission, The FCC's Proposed Voluntary Cybersecurity Labeling Program for Internet-Enabled Devices, 2023, available at: https://docs.fcc.gov/public/attachments/DOC-395909A1.pdf
[34] European Commission. The Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554.[EB/OL], 2023, https://www.digital-operational-resilience-act.com/
[35] European Commission. Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive), 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-20221227&qid=1713876904163

[36] The EU Cyber Solidarity Act, 2023, https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act
[37] US Department of Energy, National Cyber-Informed Engineering Strategy, 2022, https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf
[38] Liu ZT, et al. Systematic thinking and classified implementation of high-quality development of higher education. Univ Edu Sci 2021: 4–19.
[39] Jones KS, Namin AS and Armstrong ME. The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. ACM Trans Comput Edu 2018; **18**: 1–12.
[40] Wirfs-Brock R. The responsible designer. IEEE Softw 2009; **26**: 9–10.
[41] Knowledge, skills, and abilities for specialized curricula in cyber defense: Results from interviews with cyber professionals. ACM Trans Comput Edu 2020; **20**.
[42] Salleh KM, Nur HK, Noralfishah S, et al. Competency of adult learners in learning: Application of the iceberg competency model. Proc Soc Behav Sci 2015; **204**: 326–34.
[43] Crook C. Metacognitive abilities of learners: A study of learners' self-evaluation. Br Edu Res J 1988; **14**: 11–20.
[44] NIST, Workforce Framework for Cybersecurity (NICE Framework), 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf
[45] Baartman LKJ and de Bruijn E. Integrating knowledge, skills and attitudes: Conceptualising learning processes towards vocational competence. Edu Res Rev 2011; **6**: 125–134.
[46] Lombardi F and Fanton A. From DevOps to DevSecOps is not enough. CyberDevOps: An extreme shifting-left architecture to bring cybersecurity within software security lifecycle pipeline. Softw Qual J 2023; **31**: 619–654.
[47] Teaching Guidance Committee for Higher Schools, Ministry of Education, National Standard on the Teaching Quality of Higher Education Institutions for Undergraduates, 2017, https://jxzlglc.syist.edu.cn/uploads/file/20240402/20240402153544-2228.pdf
[48] Sixth Discipline Review Group of the Academic Degrees Committee of the State Council, First-level Disciplines Cultivation Requirements for Doctoral and Master's Degrees, Higher Education Press, 2014.
[49] Wu J. An Introduction to Cyberspace Mimic Defense. Beijing: Science Press, 2017.
[50] Wu J. Cyberspace Endogenous Security and Safety: Mimic Defense and Generalized Robust Control. Beijing: Science Press, 2020.
[51] Marilyn W. Computers as Components: Principles of Embedded Computing System Design. Morgan Kaufmann, 2022.
[52] Pearce JG. Telecommunications Switching. Applications of Communications Theory. Boston, MA: Springer, 1981.
[53] Zhong W, Wu W, An G, et al. Dissimilar redundancy structure design for carrier landing guidance computer and reliability analysis. In: Wang J, editor, Proceedings of the First Symposium on Aviation Maintenance and Management-Volume II. Lecture Notes in Electrical Engineering, Springer, Berlin, Heidelberg, 2014, 297.
[54] Wu J. Cyberspace's endogenous security and safety problem and the countermeasures. Sci Sin 2022; **52**: 1929–1937.
[55] Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J 1949; **28**: 656–715.
[56] Multivaluedness in networks: Shannon's noisy-channel coding theorem. In: IEEE Transactions on Circuits and Systems II-Express Briefs, 2021, 68.
[57] Iacona A. Gödel's incompleteness theorems. In: LOGIC: Lecture Notes for Philosophy, Mathematics, and Computer Science. Springer Undergraduate Texts in Philosophy, Springer, Cham, 2021.
[58] Ashby WR. An Introduction to Cybernetics. New York: John Wiley, 1956.
[59] Wiener N. Cybernetics, or Control and Communication in the Animal and the Machine, 2nd edn., MIT Press eBooks, 1961.
[60] Boland PJ. Majority systems and the condorcet jury theorem. J R Stat Soc Ser D 1989; **38**: 181–89.
[61] Verschuren P. Holism versus reductionism in modern social science research. Qual Quant 2001; **35**: 389–405.
[62] Meyer EF, Falkner N, Sooriamurthi R, et al. Reasoning: Logic and reasoning backwards. In: Guide to Teaching Puzzle-based Learning. Undergraduate Topics in Computer Science, Springer, London, 2014.
[63] Kossiakoff A, et al. Systems Engineering Principles and Practice. John Wiley & Sons, Inc., 2020.
[64] Neumann JV. General and Logical Theory of Automata. In: Aspray W and Burks A, editors, MIT Press Cambridge, 1987, 408.
[65] Esfeld M. Holism in cartesianism and in today's philosophy of physics. J Gen Philos Sci 1999; **30**: 17–36.
[66] Nidhra S. Black box and white box testing techniques – a literature review. Int J Embed Syst Appl 2012; **2**: 29–50.
[67] Xinhua Press, 2023 World Internet Conference Wuzhen Summit Opens in East China, 2023, https://english.news.cn/20231108/d9358db8163d4c17a94398286ec3e864/c.html
[68] Li P. Seizing the opportunity of "Digital Intelligence" reform, accelerating the transformation of the financial sector. Financ Times 2023.
[69] ESS Alliance. Cultivating Responsible Developers and Building Endogenous Secure Digital Ecosystems: The Third Symposium on Common Technologies in Cyberspace held in Xinghua, Jiangsu Province, 2023, https://www.secrss.com/articles/60353
[70] China Daily. Zhou's Plenary Speech at Wuzhen Summit: Security Should Evolve into a New Digital Infrastructure 2023, https://cn.chinadaily.com.cn/a/202311/08/WS654b4b39a310d5acd876df04.html
[71] Ye J. China Telecom's cloud network convergence lays out new ecology of network security. Commun Inf Daily 2023.
[72] Wu J. Endogenous Security and Safety empowers Cyber Engineering, Science Express, 2023.
[73] Liu G and Chen Y. The obscuration and transcendence of the nature of knowledge teaching. J Chin Soc Edu 2016: 17–21.
[74] Curry L and Docherty M. Implementing competency-based education. Collect Essays Learn Teach 2017; **10**: 61–73.
[75] Dewey J. Experience and Education. New York: Macmillan, 1938.
[76] Bandura A. Self-efficacy: The Exercise of Control. W.H. Freeman/Times Books/Henry Holt & Co, 1997.

[77] Dewey J and Jackson PW. The School and Society and the Child and the Curriculum. Chicago: University of Chicago Press, 1990.
[78] Ruth B. Enhancing and undermining intrinsic motivation: The effects of task-involving and ego-involving evaluation on interest and performance. Br J Edu Psychol 1988; **58**: 1–14.
[79] Waks LJ. Learning by doing and communicating: On Chapter 1: Education as a necessity of life. In: Waks LJ and English AR, editors, John Dewey's Democracy and Education: A Centennial Handbook, Cambridge University Press, 2017, 15–22.
[80] Adam S. Cybersecurity education goes broad: Future cybersecurity leaders need a wider set of skills and knowledge. Secur Mag 2019.
[81] Bergström P, Rönnlund M and Tieva Å. Making the transition from teacher-centered teaching to students' active learning: Developing transformative agency. In: Lippman PC and Matthews EA, editors, Creating Dynamic Places for Learning, Springer, Singapore, 2023.
[82] Cronin-Golomb LM and Bauer PJ. Self-motivated and directed learning across the lifespan. Acta Psychol 2023; **232**: 103816.
[83] Bardach L, et al. The power of feedback and reflection: Testing an online scenario-based learning intervention for student teachers. Comput Edu 2021; **169**: 104194.
[84] Bruce BC and Bloch N. Learning by doing. In: Seel NM, editors, Encyclopedia of the Sciences of Learning, Springer, Boston, MA, 2012.
[85] Kolb DA. Experiential Learning. Englewood Cliffs: Prentice Hall, 1984.
[86] Dillenbourg P. Collaborative Learning: Cognitive and Computational Approaches. New York: Elsevier Science, 1999.
[87] Schwartz P. Problem-based Learning. Routledge 2013.
[88] Seren Smith M, Warnes S and Vanhoestenberghe A. Scenario-based learning. In: Davies JP and Pachler N, editors, Teaching and Learning in Higher Education: Perspectives from UCL, UCL IOE Press, London, UK, 2018, 144–156.
[89] Enhancing student learning in cybersecurity education using an out-of-class learning approach. J Inf Technol Edu: Innov Pract (JITE: IIP) 2019; **18**.
[90] Cyber competitions: A survey of competitions, tools, and systems to support cybersecurity education. Edu Inf Technol 2023; **28**.
[91] Jiang B, et al. Digital twin-based modeling of endogenous security and safety cyber range, Netw Secur Technol Appl 2023: 10–13.
[92] Game-based learning platform to enhance cybersecurity education. Edu Inf Technol 2022; **27**.
[93] CyExec – Training Platform for Cybersecurity Education Based on a Virtual Environment. Int J Learn Technol Learn Environ 2020; **3**.
[94] Chen G. Practice and reflection on "Four-in-One" cultivation of innovative talents in cybersecurity. China Inf Secur 2023: 36–38.
[95] Brooks NG, Greer TH and Morris SA. Information systems security job advertisement analysis: Skills review and implications for information systems curriculum. J Edu Bus 2018; **93**: 213–221.
[96] Xue X. Model driven educational big data mining for enhancing europass and its enlightenment to China credit bank. Open Edu Res 2018; **24**: 112–118.
[97] Tagare D, Janakiraman S, Exter M, et al. Dispositions that computing professionals value in the workplace. In: Proceedings of the 2023 ACM Conference on International Computing Education Research–Volume 1, 2023, 270–283.
[98] Formosa P, Wilson M and Richards D. A principlist framework for cybersecurity ethics. Comput Secur 2021; **109**: 102382.
[99] Luyens SMM, et al. Student-centered instruction: inquiry-, problem-, project-, and case-based learning. Int Encycl Edu (Fourth Edn) 2023: 701–711.
[100] Wahsheh LA and Mekonnen B. Practical cyber security training exercises. In: 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2019, 48–53.
[101] Lu C. Cyberspace security dilemma and the construction of governance institution. Contemp Int Relat 2018; **11**: 52–53.
[102] Lin J. The construction of China's new engineering disciplines for the future. Tsinghua J Edu 2017; **38**: 26–35.

**Jiangxing Wu** is currently Dean of the Institute of Big Data and the Data Arena Institute, Fudan University; Professor and the Director of China National Digital Switching System Engineering and Technological R&D Center (NDSC), Chief Deputy Director & Scientist of Purple Mountain Laboratory. He is an academician at the China Academy of Engineering. His research interests include communication and information systems, computer architecture, and cybersecurity.

**Hong Zou** is Deputy Dean of the Institute of Big Data and of the Data Arena Institute, Fudan University, Shanghai. With an MSc degree in cybersecurity, his interests include cybersecurity and cybersecurity education.

**Jiaxi Chen** is currently a Research Assistant at the Institute of Big Data, Fudan University. With an MA degree in International Affairs, her research interests include cybersecurity governance and cyberspace policy research.

**Fan Zhang** is currently a Professor at China National Digital Switching System Engineering and Technological R&D Center (NDSC). His research interests include mimetic computing and mimetic defense technology, big data and artificial intelligence processing systems, and cybersecurity governance.

**Yuting Shang** is an Associate Researcher at the Institute of Big Data, Fudan University. With an MA degree in English Language and Literature, her research interests include social engineering and cognitive security.

**Xinsheng Ji** is currently the Cheif Engineer of Purple Mountain Laboratory and China National Digital Switching System Engineering and Technological R&D Center (NDSC). His research interests include 5G/6G security and cyber resilience.