# principles of cyberspace mimic defense

The human society is ushering in an era of digital economy at an unprecedented speed. The information network technology driven by the digital revolution has penetrated into every corner of the human society, creating a cyberspace which expands explosively to interconnect all things. A digital space associating both the real world and the virtual world is profoundly changing the ability of human beings to understand and transform the nature. Unfortunately, however, the security of cyberspace is increasingly becoming one of the most serious challenges in the information age, or the digital economy era. It is the greediness of man and the periodical attributes in the development of science and technology that prevent the virtual world created by mankind from becoming a pure land beyond the real human society. The world today has its "Achilles' heel", for example, unscrupulously spying on personal privacy and stealing other people's sensitive information, arbitrarily trampling on the common codes of conduct of the human society and the security of cyberspace, and seeking illegitimate interests or illegal controls.

Despite the variety of cyberspace security risks, the attackers' means and goals are changing with each passing day, imposing unprecedented and far-reaching threats to human life and production. The basic technical reasons, though, can be simply summarized as the following five aspects. First, the existing scientific and technological capabilities of human beings cannot completely get rid of the loopholes caused by defects in software/hardware design. Second, the backdoor problem derived from the ecological context of economic globalization cannot be expected to be fundamentally eliminated in a certain period of time. Third, the current scientific theories and technical methods are generally not yet able to

effectively check out the "dark features", such as loopholes and backdoors in the software/hardware systems. Fourth, the above-mentioned reasons lead to the lack of effective safety and quality control measures for hardware/software products in terms of design, production, maintenance and use management, where the cyber world gets severely polluted by the loopholes of technical products as the digital economy or social informatization accelerates, even heading towards annihilation. Fifth, the technical threshold for cyber attacks is relatively low in view of the defensive cost of the remedy. It seems that any individual or organization with cyber knowledge or the ability to detect and exploit the hardware/software vulnerabilities of the target system can become a "hacker" to trample on the guidelines on cyberspace morals or behavior wantonly.

With such a cost disparity in attack-defense asymmetry and such a large interest temptation, it is difficult to believe that cyberspace technology pioneers or market monopolies will not deliberately take advantage of the opportunities arising from globalization, for instance, division of labor across countries, inside an industry and even among product components, to apply strategic control methods, such as hidden loopholes, preserved backdoors and implanted Trojans. Then they can obtain improper or illegal benefits other than the direct product profits in the market through the user data and sensitive information under their control. As a super threat or terrorist force that can affect individuals, businesses, countries, regions and even the global community, dark features such as cyberspace loopholes have become a strategic resource, which are not only coveted and exploited by many unscrupulous individuals, organized criminal gangs and terrorist forces, but also undoubtedly used by stakeholder governments to build up their armed

forces and operations for the purpose of seeking cyberspace/information supremacy. In fact, cyberspace has long been a normalized battlefield, where all parties concerned are trying to outplay others. Nowadays, however, the cyberspace is still vulnerable to attacks, and yet not resilient to defend itself.

The majority of the current active/passive defense theories and methods are based on precise threat perception, and perimeter defense theory and model characterized by threat perception, cognitive decision-making, and problem removal. In fact, in the current situation where intelligent handset or terminal-based mobile offices or e-commerce have become the main application mode, as for the target object or the attached protection facilities, neither the intranet-based regional defense nor the comprehensive ID certification measures based on the "Zero Trust Architecture" can completely eliminate negative effects caused by the loopholes or backdoors. Thus, in view of the "known unknown" security risks or "unknown unknown" security threats, the perimeter defense is not only outdated at the theoretical and technological level, but also unable to provide suitable engineering means in practice for quantifiable defense effects. More seriously, so far we have not found any ideas about the new threat perception that does not rely on attack attributes or behavioral information, or any new defense methods that are technically effective, economically affordable and universally applicable. The various dynamic defense technologies represented by "Moving Target Defense" (MTD, proposed by an American) have really achieved good results in reliably disturbing or crumble the attack chains that make use of the vulnerabilities of the target object. However, in dealing with dark features hidden in the target system or unknown attacks through the hardware/software backdoors, there still exists the problem of ineffective mechanisms. Even if the underlying defense measures and mechanisms

such as encrypted authentication are used, the risks of bypass, short circuit or reverse encryption brought by dark functions from the internal vulnerabilities/backdoors of the host object cannot be completely avoided. The WannaCry, a Windows vulnerability-based ransomware, discovered in 2017 is a typical case of reverse encryption. In fact, the technical system based on the perimeter defense theory and qualitative description has encountered more severe challenges in supporting either the new "cloud-network-terminal" application model or the zero-trust security framework deployment.

Research results in biological immunology tell us that a specific antibody will be generated only upon multiple stimulations by the antigen, and specific elimination can be performed only when the same antigen re-invades the body. This is very similar to the existing cyberspace defense model, and we may analogize it as "point defense". At the same time, we also notice that a variety of other organisms with different shapes, functions and roles, including biological antigens known as scientifically harmful, coexist in the world of vertebrates. However, there is no dominant specific immunity in healthy organisms, which means the absolute majority of the invading antigens have been removed or killed by the innate non-specific selection mechanism. The magic ability obtained through the innate genetic mechanism is named non-specific immunity by biologists, and we might as well compare it to "surface defense". Biological findings also reveal that specific immunity is always based on non-specific immunity, with the latter triggering or activating the former, while the former's antibody can only be obtained through acquired effects. Besides, since there are qualitative and quantitative differences between biological individuals, no genetic evidence for specific immunity has been found to date. At this point, we know that vertebrates acquire the ability to resist the invasion of known or unknown

antigens due to their point-facet and interdependent dual-immune mechanisms. What frustrates us is that humans have not created such a "non-specific immune mechanism with clean-sweep properties" in cyberspace; instead, we always try to address the task of coping with surface threats in a point defense manner. The contrast between rational expectation and harsh reality proves that "failure in blocking loopholes" is an inevitable outcome, and it is impossible to strategically get out of the dilemma of dealing with them passively.

The key factor causing this embarrassing situation is that the scientific community has not yet figured out how non-specific immunity can accurately "identify friend or foe". According to common sense, it is impossible for the biological genes, which cannot even carry the effective information generated from biological specific immunity, to possess all the antigenic information against bacteria, viruses and chlamydia that may invade in the future. Just as the various vulnerability/attack information libraries in cyberspace based on behavioral features of the identified backdoors or Trojans, it is impossible for today's library information to include the attributes of backdoors or Trojans that may be discovered tomorrow, not to mention the information on the form of future attack characteristics. The purpose of our questioning is not to find out how the creator can endow vertebrate organisms with the non-specific selection ability to remove unknown invading antigens (the author believes that with the restraint of operational capability of the biological immune cells, the method of coarse-granule “fingerprint comparison”may be used based on their own genes and all the invading antigens not in conformity with the genes will be wiped out. As an inevitable cost, there exists a low probability of some “missing alarms, false alarms or error alarms” in the coarse-granule fingerprint comparison. Otherwise vertebrate biological beings will not fall ill or suffer from cancers. And it

would be unnecessary for extraordinary immune powers to exist. The comparison of own credibility and reliability is a prerequisite for the efficacy of the comparison mechanism, but with an unavoidable risk. ), but to know whether there is a similar identification friend or foe (IFF) mechanism in cyberspace, and whether there is a control structure that can effectively suppress general uncertain disturbances, including known unknown risks and unknown unknown threats, to obtain endogenous security effects not relying on (but naturally converging with) the effectiveness of any attached defense techniques. With such mechanisms, structures and effects, the attack events based on vulnerability backdoors or virus Trojans can be normalized to conventional reliability issues. In accordance with the mature robust control and reliability theories and methods, the information systems or control devices can obtain both stability robustness and quality robustness to manage and control the impact of hardware/software failures and man-made attacks. In other words, it is necessary to find a single solution to address the reliability and credibility issues at both the theoretical and methodological level.

First, the four basic security problems in cyberspace are generally regarded as the restrictive conditions because the basic security problems will not change when the system host or the attached or parasitic organizational forms change or when system service functions alter. Hence we can come up with three important conclusions: security measures may be bypassed in the target system with shared resource structure and graded operational mechanisms; attached defense cannot block the backdoor function in the target object; defense measures based on priori knowledge and behavior information and features can not prevent uncertain threats from unknown vulnerabilities and backdoors in a timely manner.

Secondly, the challenge to be conquered is how to perceive unknown

unknown threats, i.e. how to achieve the IFF function at low rates of false and missing alarms without relying on the priori knowledge of attackers or the characteristics of attack behaviors. In fact, there is no absolute or unquestionable certainty in the philosophical sense. Being "unknown" or "uncertain" is always relative or bounded, and is strongly correlated to cognitive space and perceptual means. For example, a common sense goes like this: "everyone has one shortcoming or another, but it is most improbable that they make the same mistake simultaneously in the same place when performing the same task independently" (the author calls it a "relatively correct" axiom, and the profession also has a wording of the consensus mechanism), which gives an enlightening interpretation of the cognitive relationship of “unknown or uncertain” relativity. An equivalent logic representation of the relatively correct axiom—the heterogeneous redundant structure and the multimode consensus mechanism, can transform an unknown problem scene in a single space into a perceptible scenario under the consensus mechanism in a functionally equivalent multidimensional heterogeneous redundant space, transform the uncertainty problem into a reliability problem subject to probability expression, and transfer the uncertain behavior cognition based on individuals to the relative judgment of the behavior of a group (or a set of elements). In turn, the cognitive or consensus results of the majority are used as the relatively correct criteria for reliability (this is also the cornerstone of democracy in human society). It should be emphasized that, as long as a relative judgment is made, there must be a "Schrodinger cat" effect like the superposition state in quantum theory. “Right” and “wrong” always exist at the same time, while the probability is different. The successful application of a relatively correct axiom in the field of reliability engineering dates back to the 1970s, when the first dissimilarity redundancy structure was proposed in flight controller

design. For a target system based on this structure under certain preconditions, even if its software/hardware components have diversely distributed random failures, or statistically uncertain failures caused by unknown design defects, they can be transformed by the multimode voting mechanism into reliability events that can be expressed with probabilities, enabling us to not only enhance system reliability by improving component quality but also significantly enhance the reliability and credibility of the system through innovative structural technology. In the face of uncertain threats exploiting the backdoors of the software/hardware system (or man-made attacks lacking in priori knowledge), the dissimilarity redundancy structure also has the same or similar effect as the IFF. Although the attack effect of uncertain threats is usually not a probability problem for heterogeneous redundant individuals, the reflection of these attacks at the group level often depends on whether the attacker can coordinately express consensus on the space-time dimension of multimode output vectors, which is a typical matter of probability. However, in a small-scale space and a certain time, a target object based on the dissimilarity redundancy structure can suppress general uncertain disturbances including unknown man-made attacks, and has the quality robustness of designable calibration and verification metrics. However, the genetic defects of the structure, such as staticity, similarity and certainty, mean that its own backdoors are still available to some extent, where trial and error, exclusion, common model coordination and other attack measures often corrupt the stability robustness of the target object.

Thirdly, if viewed from the perspective of robust control, the majority of cyberspace security incidents can be considered as general uncertain disturbances arising from attacks targeted at the backdoors or other vulnerabilities of target objects. In other words, since humans are

not yet able to control or suppress the dark features of hardware/software products, the security and quality problems, which originally arise from the design or manufacturing process, are “forced to overflow” as the top security pollution in cyberspace due to “the unconquerable technical bottleneck.” Therefore, where a manufacturer refuses to promise the safety and quality of its software/hardware products, or is not held accountable for the possible consequences caused thereby, seems that it has a good reason to justify its behavior by the "universal dilemma". In the era of economic and technological globalization, to restore the sacred promise of product quality and the basic order of commodity economy, and fundamentally rectify the maliciously polluted cyberspace ecology, we need to create a new-type of robust control structure that can effectively manage and control the trial-and-error attacks, and the uncertain effect generated by the feedback control mechanism driven by the bio-mimic camouflage strategy, providing the hardware/software system with stability robustness and quality robustness against general uncertain disturbances.

Furthermore, even if we can't expect the endogenous security effects of the general robust control structure and the mimic camouflage mechanism to solve all cyberspace security problems, or even all the security problems of the target object, we still expect the innovative general robust structure to naturally converge with or accept advances in existing or coming information and security technologies. Whether the technology elements introduced is static or dynamic defense, active or passive defense, the target object's defense ability should be enhanced exponentially so as to achieve the integrated economic and technological goal of “service-providing, trusted defense and robustness control.”

In order to help readers better understand the principles of cyberspace mimic defense, the author has summarized its key theoretical

points into the following: one revolving premise (unknown vulnerabilities and backdoors in cyberspace can lead to uncertain threats); one theory-based axiom (conditional awareness of uncertain threats can be provided); discovery of one mechanism ( with the self-adaptable mechanism of “non-decreasing initial information entropy”, uncertain threats can be stably prevented.) ; invention of one architecture (the dynamical heterogeneous redundant architecture DHR with the general robust control performance has been invented); introduction of one mechanism（mimic guise mechanism）; creation of one effect (difficult to detect accurately); achievement of one function(endogenous security function) ; normalization of dealing with two problems simultaneously( making it possible to provide an integrated solution to the problems of conventional reliability and non-conventional cyber security )； production of one non-linear defense gain (introduction of any security technology can exponentially promote defense effects within the architecture. )

Finally, it is necessary to complete the full-process engineering practice through the combination of theory and application, covering architecture design, common technology development, theoretical verification, application piloting and industry-wide demonstration.

"Cyberspace mimic defense" is just what comes out from the iterative development and the unremitting exploration of the above-mentioned ideas.