

# THE CREATOR DESTROYER METHOD - AN EXPLORATION INTO A NON-RATIONAL APPROACH OF RED TEAMING

DOI: <https://doi.org/10.37458/nstf.25.2.1>

Original scientific paper

Received: October 31, 2024

Accepted: December 5, 2024

**Djie Han Thung, Willem Leeuwenkamp, Giliam de Valk\***

**Abstract:** In this article, we focus on a new perspective for asymmetric red teaming. In asymmetric red teaming, there are two issues that are problematic to deal with. Firstly, to red team it is advised to bring in external people for a fresh view, but this may cause problems for reasons of sensitivity. Secondly, although creativity is highly valued, there is an implicit rationality bias in the thinking of most professionals.

---

\* Djie Han Thung is a filmmaker, designer, and lecturer/researcher at the department of Communication and Multimedia Design at the Amsterdam University of Applied Sciences. Thung has developed a design method aimed at foreseeing unknown, unexpected, undesired aspects of a (security) design.

Willem Leeuwenkamp is a senior intelligence consultant at SoSecure Netherlands. At SoSecure, he leads and executes various red teaming projects and develops intelligence techniques and proactive security methods. He also provides training for professionals within the security sector.

Giliam de Valk is specialized in the methodology of security and intelligence analysis. He is an assistant professor at the Institute for Security and Global Affairs, Leiden University. In 2021, he has won the Tudjman Scientific Excellence Award of the Zagreb Security Forum.

In the Netherlands, a method has been developed – and tested – that has a high potential to address both issues at the same time. Firstly, the exercise is designed such that it will detach the security officers from their daily routine and thinking. As part of it, the participants have to invent – and play – a mythical persona, with mythical powers, that are a threat for the interests they must protect. This approach will get the officers out of their daily routine, and lead to a free way of thinking – detached from their daily work. Above that, the mythical powers of their persona trigger a creative approach on finding possible new modus operandi. This way, the first issue – just to work with your own team and at the same time come to fresh creative views as if you are an outsider – can be addressed.

Secondly, also the rationality bias will be addressed. By developing and playing mythical persona, the process of creativity taps in into a deeper, subconscious, level. You tap in to the deeper level of archetypes and non-rationality. The participants can leave behind their rationality bias that permeates the western (labor) culture.

Thirdly, an extra element has been built in the method. By handing out cards, the participants are asked to reflect on certain emotions and sins in the context of their security issue. It leads to an additional layer of creativity on top of the other ones. In one of the exercises, for example, a participant drew the card on vanity. The outcome was that if someone like a prime minister would visit the organization, the head of security would not leave the welcoming to the subordinates, as it should be conforming the protocol. The head of security would personally come downstairs instead to welcome this guest, as this visit would be the career highlight. Meaning that when the stakes are the highest – the most vulnerable guests possible are visiting your organization – the coordinator is not in place when something happens.

The exercise can be carried out within two hours. If a guided come-back-hour within a week is held, this will lead to additional results. The method needs special attention in the way it is carried out.

Firstly, the framing of the exercise – before the actual exercise is started – is crucial. Only then the free-thinking process really takes off. Secondly, during the exercise, the facilitator of the exercise never at any moment interferes with the contents of the process.

**Keywords:** red teaming, security design, non-rationality, irrational unknowns, residual threat.

## ***Introduction***

Global geopolitical tensions, societal polarization, and flourishing organized crime have significantly increased threats to individuals and organizations. Recent incidents in the Netherlands indicate that terrorist and criminal groups, as well as hostile intelligence services, have become more assertive in threatening critical persons and vital infrastructure. The 2024 attacks on presidential candidate Donald Trump underscore that even the most heavily guarded individuals are not immune to threats. Consequently, the security of such high-profile targets must be proactively addressed, emphasizing on broad situational awareness and the identification of (new) modus operandi and warning indicators (Berkowitz, 2008; Borum, et. al., 1999).

In the security domain, red teaming is a widely used method to test the protection of objects, persons and systems. It is primarily oriented to identify new modus operandi, before an opponent will do so. Two limitations return in the practitioners' literature. Firstly, it is needed to include outsiders in the exercise as this will provide a fresh perspective on the case. However, sometimes this is problematic for reasons of sensitivity. Secondly, professionals tend to have – for good reasons – a rationality bias. This bias can cause a blind spot of threats that remain unnoticed. We will deal with a new

perspective for red teaming and we will address both issues – only to include the own security personnel and to minimize the rationality bias.

But before we start elaborating this new approach, we will reflect on what red teaming is. Often there is confusion on the use of the term ‘red teaming’. Is it on the strategic level, or is it on the tactical and operational level? Is it a tool of wargaming, or is it about security and the protection of objects persons or systems? This confusion is largely due to the two main purposes that red teaming is used for – symmetric red teaming and asymmetric red teaming.

### ***The roots of Red Teaming***

Symmetric red teaming started in the United States of America (USA) as a tool for wargaming during the cold war. Red was the color of the opponents – the Union Soviet Socialist Republic (USSR) and the Peoples Republic of China (PRC) – and the North Atlantic Treaty Organization (NATO) were the blue forces. One NATO team would then play the role of the opponent – the Red Team.

At its latest at the end of the 1950’s, the first military manuals appeared that clearly gave direction to this kind of exercises (Department of the Army, 1959). In 2004 - in the aftermath of two big intelligence failures- through the Intelligence Reform Act, it was formalized that red teaming should be installed as a tool in the decision-making process (USA, 2004).

In symmetric red teaming, four principals can be distinguished – self-awareness and reflection, groupthink mitigation and decision support, fostering

cultural empathy, and applied critical thinking (University of Foreign Military and Cultural Studies, 2018). It helps to obtain a fuller picture of the opponent, to identify the intelligence demands, and to incorporate it into the decision-making process.

In the manuals special attention is given to the team composition with, among others, persons with a relevant cultural background from countries of the opponent. The outcomes are not limited to the primary reactions, and it is largely an intellectual process (University of Foreign Military and Cultural Studies, 2018). Red teaming turned out to be helpful tool to identify vulnerabilities, before the opponent can do.

Asymmetric red teaming, carried out in a civilian context, was both preceded by and evolved from the military symmetric red teaming – in which also security measures are tested and evaluated. Asymmetric red teaming was also preceded by Structured Analytical Techniques to identify vulnerabilities in security measures. Such methods could be used to tests physical, technical, or human aspects of security. And thus, could also have been part of a bigger symmetric red team exercise. But it can be used independently as well. Red Teaming falls under the category of alternative intelligence techniques, to contradict worn in world views.

Two examples of such preceding techniques are the Fault Tree Analysis and the Quantitative Intrusion Path Analysis. The Fault Tree Analysis was developed as a failure-oriented technique to assess the reliability of a technical system, but it can be applied more broadly. It is a top-down approach to make an inventory of all the

composing parts that may lead to a failure (DeLong, 1970). Quantitative Intrusion Path is designed to weigh (to assess) both physical security measures and the human factor. It measures if an opponent could enter – and at what speed, and by what modus operandi – a secured object of the critical infrastructure. It measures the delay by physical barriers, and calculates issues as recognition, warning and reaction time (Proliferation Resistance and Physical Protection Evaluation Methodology Working Group, 2009).

The prime characteristics of these techniques are to assess and to make an inventory. Although it is helpful to get an inventory of all the elements in play – together with a ring model to calculate delay – the later asymmetric red teaming had a different focus. Firstly, contrary to Fault Tree Analysis and Quantitative Intrusion Path Analysis, asymmetric red teaming primarily focusses on to identify new modus operandi. Secondly, where Fault Tree Analysis and Quantitative Intrusion Path Analysis make an inventory and calculation of the vulnerabilities, red teaming primarily focusses on how to monitor the emerging threat in its evolving steps.

Israel played an important role in developing this new approach of asymmetric red teaming. Asymmetric red teaming was integrated in the proactive security methodology. The proactive security methodology known as Predictive Profiling was developed in Israel to identify and mitigate potential threats at an early stage, prior to the occurrence of incidents. The approach involves the capability of security profilers to assess threats arising from situations, individuals, or objects based on warning signs associated with a specific modus

operandi (Van der Plas & Leeuwenkamp, 2018). The distinction in the execution of this method lies in understanding of the specific adversary that is being examined, along with their unique modus operandi and associated warning indicators. Subsequently, through organizations such as Chameleon, asymmetric red teaming and the proactive security methodology was shared with and spread throughout the world.

### ***A shift in methodology***

The Israeli innovations in asymmetric red teaming were no less than a methodological revolution. In the US approach, the dominant element is to assess. We can see this in the reliance on Structured Analytic Techniques (University of Foreign Military and Cultural Studies, 2018) – including the preceding techniques of Fault Tree Analysis and Quantitative Intrusion Path Analysis. It is on to assess the reliability of a system, and to assess how long it takes to pass barriers. Also, in other NATO techniques on threats identification that are originated in the US, we can see this emphasis on assessment – like in early warning in which it is assessed by critical indicators if a certain warning scenario takes place (De Valk, 2023).

All these techniques are designed to assess a threat in the first place. The methods are designed such that it is aimed at to minimize a wrong assessment. A wrong assessment is related to your Type-1 errors – that you make an incorrect relationship. The US methods mentioned are primarily meant to reduce those Type-1 errors. In the US approach, you want the assessments to be correct as possible. It reduces your tolerance for your

Type-1 errors. Or in other words, it reduces the value of your  $\alpha$  (De Valk & Goldbach, 2020).

The Israeli approach is methodologically radically different. It is primarily oriented at to refute. In this red teaming technique suspicious indicators are developed. If such a suspicious indicator is monitored, it is tried to refute that it is related to that threat. By having suspicious indicators, you do not want to miss any threat in the first place. The red team exercise itself is aimed at to identify new modus operandi. This emphasis on identifying new modus operandi is also aimed at that you do not want to miss any threat in the first place. To miss a threat is related to your Type-2 errors. The Israeli techniques are primarily oriented at reducing your Type-2 errors. In the Israeli approach, you don't want to miss a threat in the first place. It reduces your tolerance for your Type-2 errors. Or in other words, it reduces the value of your  $\beta$  (De Valk & Goldbach, 2020). As red teaming is on discovering unknown-unknowns – not to miss a threat – it explains the popularity of the Israeli innovations in asymmetric red teaming.

### ***Blind spots in asymmetric Red Teaming: internal teams and rationality bias***

Asymmetric red teaming focuses on identifying new modus operandi and how to monitor these threats in different stages of its evolving steps. It is a process in which experts test the security and effectiveness of an organization or system by simulating realistic attacks from the perspective of an adversary. The goal is to identify vulnerabilities, suggest improvements and enhance the organization's resilience. By structurally employing red teaming, organizations can improve their



decision-making and operational processes, uncover residual threats, and train employees to respond effectively to threats.

If we would put this asymmetric red teaming in a broader context of a threat and security analysis, it could be described as a semi-unstructured experiment, in which both method and data are not known yet. In that sense, it is an unknown (method) unknown (data) approach (De Valk, 2018).

In asymmetric red teaming it is advised to work with outsiders for a fresh view to get new perspectives. Yet, some security issues are so sensitive, that you don't want to share your secrets with outsiders. This could hamper the fresh perspective. Besides, as mentioned, red teaming is described as largely an intellectual process – which is a filter as such. It may lead to a rationality bias – which may become bigger if it is carried out by the own security professionals.

In our proposed method, it is aimed at to cope with both these issues – just the own people and rationality bias. If we would describe red teaming as identifying residual threats, our method can be described as facilitating in uncovering the blind spots in these residual threats. By that, we can diminish the residual threat even further and at the same time keeping things secret that do not need to be shared.

Or, if we formulate it from the perspective of a team of security officers: how do we get our officers out of their daily routine, and out of their rationality bias in which rationality is part of their attitude and profession? In the next part – on the Creator Destroyer method – we will share our first experience with experiments with this

method. It led to promising outcomes, even while exercises only lasted for two hours.

### ***The Creator Destroyer method: introduction***

The Creator Destroyer method originally has been designed as a method for designers to mitigate unknown unexpected effects of a design. It was developed by – and experiment with – Djie Han Thung. From the starting point it has been aimed at designers in the broadest sense, not only product designers but also system and organizational designers. In the development of this method, it has therefore not only been tested on designers and design students, but also on security designers.

Starting point of most design methods is to be scientific and rational, two aspects that have become synonymous in western society since Descartes (Malik, 2002). As a result, we use rational design methods like Personas (Cooper, 1992) and Empathy Maps (Gray, 2010) which are focused on the goals of the design and the intention to improve the current situation with the design. This rational approach of design has led to the present situation where data is not only used to analyze past events, but the resulting model of reality is valued higher than reality, and this virtual model is used to shape the present and the future (Bridle, 2018).

Recent affairs like the Post Office scandal in the U.K. and the Child Benefit scandal in the Netherlands have shown, how these logical designs can have disastrous results for the people involved. Logic and reason are no guarantees for design that is good for the world we live in. In general design methods are intended to do good as

a leading principle. However, very human traits like lust, envy and hate are mostly ignored in design methods.

In contrast, games, films, series, and books in which these urges are central to the story or characters involved, are hugely popular, as can be seen in their rankings in the charts. The popularity of these kinds of entertainment, shows that although most people probably intend to do good. There is a longing for the exploration of unwanted needs and feelings. In the early twentieth century Carl Jung, the founder of analytical psychology already found that to be complete and whole, we must acknowledge our Shadow, the dark aspects in ourselves (Jung, 1951), This duality of the whole has been described centuries earlier in Chinese philosophy in the form of the Yin Yang. The concept of opposing but interconnected forces that complement each other.

This part of being human, our dark half, is ignored in most modern design methods. In contrast with our professional behavior, we seem to explore this darker side of life happily in entertainment. By ignoring this part of ourselves in design methods and rationally focusing on the purpose of the design, we not only reduce the world to a rational system, but we also create a blind spot for unintended unwanted effects of a design that are not within this scope.

### ***The Creator Destroyer method: the unknown-unknown and non-rationality***

The blind spots created by our rational focus form part of the “Unknown-Unknown”, things we do not know we do not know. The Unknown Unknowns are an element of the Knowledge Matrix, originally called the Johari window, a psychological tool (Luft, 1955). Now

it's commonly used in risk assessment and intelligence operations to map threats. The quadrants of the Knowledge Matrix represent the four parts of what we need to know for threat mitigation.

There are the Known Knowns, the things we know we know. The Known Unknowns, refer to things we not realize we know. These this can be identified through research. The Unknown Knowns refer to the things we do not realize we know. These we also must re-discover while researching. Finally, the Unknown Unknowns, or the things we do not know that we do not know, lie beyond the scope of our objectives and ways of thinking.

The Unknown Unknowns are potentially the most dangerous element of the knowledge as we probably cannot uncover them with our regular methods due to being outside the realm of rational thought. Even more worrying is that they pose significant threats. What lies in the realm of the Unknown Unknowns can be the cause of so-called Black Swan events, highly unexpected unforeseen occurrences with enormous impact for society and the world (Taleb, 2007). Communication designs like TikTok and Facebook have shown us how designs can have a far-reaching unexpected impact on society, the way we see ourselves and others and the way we behave, which has led to division, addiction, riots and even genocide (Amnesty International, 2022). By using the appeal of undesired human urges, that are ignored in current design approaches, we might be able to uncover and mitigate unforeseen harmful effects that conventional approaches miss.

There exists within us the desire to make sense of the things we cannot control and that are out of reach of our

logical understanding, often sparking creativity to come up with fantastical stories that explain the unknown. Even in our so called modern, rational societies, this need for sense making persists, and seems to fulfil a deep grounded human urge. A need for meaning where there might be no meaning. In the way our modern institutions are organized based upon reason, the sacred, the ritualistic, magical, religious part of life is neglected (Habermas, 2011). Mythical stories, are related to the uneasiness and dangers in the society and culture where they emerge (Musharbash, 2018). Studies of conspiracy theories have shown these conspiracy theories have a remarkable likeness to folktales (Tangherlini, 2018). In these mythical stories, dangers and threats are creatively connected with invisible powers that are beyond our control. In the unknown everything is possible and the way to get there can go in every direction. In a mindset where science and reason play no part, our attention can go unhindered in any direction. Designers might foresee these irrational reactions and consequences of their designs when they, as designers, use their own irrational feelings and fears in design methods.

To explore this concept, a method using embodiment, play, and mythical storytelling has been designed. As this method shifts (security) designers from a creating into a destroying objective, is called ‘Creator-Destroyer’, referring to the creatures in mythical stories around the world that represent duality and are not only the creator of worlds but also its destroyer (Buenfeld, 2020).

### ***The Creator Destroyer method: design***

In this method, participants are tasked with creating a world and costumes for imagined mythical creatures. In the role of these creatures, participants must think of ways their design could be corrupted or perverted. Masks serve as a tool in the process, facilitating a shift in perspective by enabling to adopt into a malignant perspective of a malevolent creature. The use of masks has a close connection to the understanding of identity, to impersonate the other and to express all kinds of longings and feeling (Mathieu, 2017).

To ease participants into wearing masks of malignant mythical creatures, the exercise is designed to take the participants there gradually, using principles of worldbuilding. The concept of worldbuilding is to create a believable, immersive narrative by first designing a consistent world (Stackelberg, 2015). This approach aligns with theories on worldview, the way we view the world and what we believe and find acceptable. One of the aspects that establishes this worldview is based upon the ontological aspect, that which we see as the truth is based upon the relation of the things we perceive (Hall, Hill, 2019). So, to help the participants getting into a mindset in which they could enter a different world with different rules the method starts with literally, physically creating a world. In transition from thinking to doing brings the people into a mindset where they are becoming more playful (Huizinga, 1938). The method is designed with a series of distinctive steps that leads participants into a state of play by creating their own magic circle, a world with its own internal logic separated from daily life (Huizinga, 1938).

This method is intended for a team of (security) designers working on the same project. The only preliminary briefing they receive is that they will participate in a process aimed at discovering unknown threats. After this the team gathers in a room with enough space for movement and activity, equipped with lots of cardboard, a working table, paper and utensils for drawing cutting and assembling.

**Step 1: Creating the world.** The participants are provided with a round piece of cardboard, along with paper, cardboard, tape, glue, pencils, and markers. They are instructed to use these materials within ten minutes to create a world where their design would exist. The assignment: You have ten minutes to create a world where your intended (security) design will exist, using paper, cardboard, tape, glue, pencils and markers. Build this world on the given round piece of cardboard.

**Step 2: Drawing the creature.** Each participant is given each a blank A4 paper and instructed as follows: ‘The world you have created, is a world like any other world, with people who believe in myths about creatures living in the forests that have the power to influence and manipulate the people. Imagine and draw such a mythical creature that inhabits the woods. You have five minutes to write down its name and the special malignant powers it possesses.’

**Step 3: Creating masked costumes.** To reinforce the idea that participants are now inhabiting the world they have created, they receive the following instructions: ‘All over the world we see that during festivities and rituals, people make costumes and masks to impersonate these kinds of mythical creatures. Could you make a

costume and a mask you could wear, to impersonate your creature, using cardboard, tape, glue, pencils, and markers? You have ten minutes.’

**Step 4: Wearing the costumes and impersonating the creatures.** The participants are asked to wear their masked costume and to act out the creature they have created, demonstrating its posture, movement and powers one by one. The assignment: Put on the costume and the mask. Now could you show, how this creature moves and acts, and how it uses its powers?



Step 4. Participants wearing their masks and impersonating their creature

**Step 5: Conspiring.** The participants are asked to remain in character. In this state they must conspire together on how their creatures could undermine and pervert the (security) design. The assignment: Remain in character and keep your costume and mask on. Place the world you created on the floor and gather around it. Now conspire together with your team, each of you in character of your creature, and think of ways how your character could pervert or breach your security design.








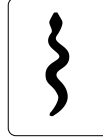

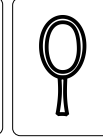

Step 5. Participants conspiring

**Step 6: Seven Sins cards.** The participants are presented a set of seven cards, each representing one of the seven deadly sins. The back of the cards only shows symbols, making the content unpredictable and the cards are drawn in random order. The participants are asked to draw one of the seven sins cards and imagine in which ways this motivation could have a negative impact on the design. This is repeated with a couple of cards.

**Step 7: Evaluating.** The experience and the outcomes are evaluated in two steps. In the first step the participants fill out a systematic questionnaire based on Gibbs' Reflective Cycle (Gibbs, 1988). In the second step reflection occurs in group discussion, with questions such as; What are the concrete results? What are potential effects of the experience for future approaches? How can the creature and its powers be transformed from a metaphorical form to a concrete threat?

**Step 8. Reflection.** This phase focuses on the operationalization. In this phase participants are asked to consider how to translate the metaphor of their creature

and its powers into a credible threat by viewing the creature as a symbol for a real-world danger.

						
<p><b>Lust</b></p> <p>The sexual desire. How can this cause danger for your security design.</p>	<p><b>Wrath</b></p> <p>The desire to be vindictive. How can this cause danger for your security design.</p>	<p><b>Gluttony</b></p> <p>The desire to indulge in food, drink, or drugs. How can this cause danger for your security design.</p>	<p><b>Envy</b></p> <p>The desire to destroy another's quality, skill, achievement, or possession. How can this cause danger for your security design.</p>	<p><b>Greed</b></p> <p>The desire for power, wealth, or possessions. How can this cause danger for your security design.</p>	<p><b>Vanity</b></p> <p>The love for one's own achievements and appearance. How can this cause danger for your security design.</p>	<p><b>Sloth</b></p> <p>The desire to be idle. How can this cause danger for your security design.</p>

Step 6. Seven Sin cards. Top: back with symbols. Bottom: front with instruction to use certain sin as motivation



Step 7. Gibbs' Reflective Cycle

## ***The Creator Destroyer method: insights from the experiments***

The Creator Destroyer method was tested with various groups of designers. A total of 68 participants took part in 13 different sessions, divided into 18 teams, including:

- a team of bachelor students in Interaction Design (2 students);
- nine teams of bachelor students in Service Design (27 students);
- four teams of master students in Applied A.I. (16 students);
- a team of designers from a design company (5 designers);
- a team of security service professionals following a course on Radicalisation and Terrorism (6 people of different security institutions)
- two teams of security coordinators from the Dutch Government (12 civil servants).

The first sessions were evaluated by interviewing the participants. Subsequently, a structured evaluation form was introduced, which provided deeper insights into individual experiences. The participants filled out reflection forms directly after the exercise. Once these forms were filled out, a group interview was conducted. This led to richer insights, as participants had already formulated their thoughts by filling out the structured forms.

Across all sessions, with all the different groups of people, all participants got into making and acting. Although the level of enthusiasm about the exercise varied, the results showed that even the most hesitant participants got into a creative mode of making and acting.

## ***Evaluation step by step***

**Step 1: Creating the world.** After having received the instructions to build the world, participants often had clarifying questions, such as: What do you mean with the world? Is it the location where the target group is? Do you mean the surroundings or the thing we are making? They were told that their world could be as big or as small as they wanted, as long as it provided a setting for (security) design. The participants were purposely given no clue of what the objective was of building this world. The idea was to have them start making without overthinking it rationally, as they only had ten minutes. The results varied from very detailed miniature scenes like a fenced building with a bomb exploding on the roof, to more abstract settings, such as roads and buildings or even a theoretical representation. In general, as the participants were building the world, the conversations were very much focused on the real world, of the setting and the actors involved as they had mapped them. This was confirmed in the post-exercise reflection forms and group discussion.

**Step 2: Drawing the creature.** The second step, in which participants were asked to imagine and draw a mythical creature, took them by surprise as it seemed to have nothing to do with their design. Most of them started drawing and writing very quickly. Some of the participants initially seemed a bit at loss with this assignment, but under the pressure of the five-minute time limit they eventually started writing and drawing. This was the turning point where the participants were starting to have fun and started joking about the things they came up with. This was the moment where they started to stop thinking about the goal and the meaning

of the exercise and just started to draw and write whatever came up, without thinking about results.

**Step 3: Creating masked costumes.** By the third step, participants became fully absorbed in the activity. They started making the masked costumes and were creating all kinds of details and finding solutions to transform their ideas of the creature into a costume.

**Step 4: Wearing the costumes and impersonating the creatures.** Although the participants were specifically instructed to make a masked costume they could wear, the process of making seemed to have gotten them into the state of making so much, that when asked to wear the costume and act out their creature, most of the participants were initially slightly shocked. Apart from one participant, they all put on their masked costume and showed how their creature acted and moved. Whereas most of them showed this simply by posture and movement, some of them really got into it by producing aggressive roaring sounds and pretending to attack.

**Step 5: Conspiring.** During the conspiring phase, participants were asked to remain in character and devise ways to corrupt or subvert the (security) design. However, rational thought seemed to return during this step, and many participants found it challenging to stay in character. As a result, fewer original ideas emerged during this phase.

**Step 6: Seven Sins cards.** During the sessions with the security coordinators, an interesting insight popped up. After picking one of the seven sins cards – the one on vanity – a security issue was discussed that was previously overlooked. The result showed that if a high profile figure such as the prime minister would visit their

organization, the head of security would deviate from protocol and welcome the guests, as this visit would be the career highlight. Meaning that when the stakes are the highest, the head of security might be distracted or absent from their post and is not able to intervene when a crisis situation happens.

**Step 7: Evaluating.** In the final evaluation phase, participants were asked to think of a way to translate their creatures and its powers into a credible real-world threat, by seeing the creature as a metaphor for something real. This led to a few practical ideas and provided the participants with more tangible, concrete results. The reflections of the participants afterwards showed something very interesting had happened during these sessions. Participants realized that their understanding of the context in which their design operated had been more limited than they thought. The experience of performing the method, created or heightened their awareness of the wide-ranging impact that a design could have in the world as unity of interconnected actors, and not only within the context of the researched situation and its stakeholders.

**Step 8. Reflection.** Reflecting on the positive outcomes of step 6 – the Seven Sins cards, a new iteration of the method was developed. In this version, an operationalization phase was introduced after the evaluation forms were filled out. In this phase the participants were asked to think of a way to translate the idea of their creature and its powers into a credible threat, by seeing the creature as a metaphor for something real. We implemented this in the following session. This gave two improvements. Participants could translate the powers of some of their creatures into real

world situations. And it gave the participants an outcome they were more accustomed to in the way of more tangible, concrete results. Since step 8 was introduced only later in the research process, this step was only tested with a limited number of participants.

### ***General observations***

There were no big differences between these different groups in the way they underwent the method. Overall, most participants enjoyed the experience and felt that the method had given them new perspectives. The immediate results varied, some participants indicated that they obtained new insights that directly influenced the design they were working on, while others stated that it opened ways of thinking that could be useful in the future.

The biggest difference turned out to be whether a team was in a room together with other teams or whether there was just one team present. In reflection afterwards the participants who shared the room with other teams felt that the presence of the others had held them back. The presence of an instructor did not seem to bother the participants, as long as the instructor kept a distance from the worktable. Another finding was that written instructions tended to cause more confusion than oral instructions.

One of the most interesting results was that the method made participants realize that their perspective on the context had been more limited than they thought. The experience created or heightened their awareness of the wide-ranging impact that a design could have in the world as a whole of interconnected actors, and not only within the context of the researched situation and its

stakeholders. The building of the world and thinking of unusual external characters and how they would interact in this world and with the people in it, helped them getting this broader perspective. Although they had previously worked with methods to map the broader context, these methods were often still goal oriented and practical, which limited their scope, as they now realized.

In every group there were some participants who started out quite reserved and who were clearly sceptical about the imaginary direction the method was going. Sometimes this resulted in minimal participating in the first step of world-building. However, when asked to think individually and draw a mythical creature, they, like the others, literally seemed to get drawn into the world they had created. In fact, some of the most sceptical individuals ended up being the most engaged, jumping off the couch or crawling on the floor while acting out their creature.

The reflections and interviews afterwards showed that participants struggled initially with letting go of rational thinking and the research methods they were accustomed to. The methods they were used to were aimed at making the design better, whether it be through understanding the actors involved, the context, or the working itself. In their minds a design method had to be useful in the sense that it would be aimed at the intended use and would generate useful outcomes that could be implemented in the design on a practical way. This framing of design methods as a utilistic, rational tool resulted in some participants even saying the Creator-Destroyer method was unrealistic or not scientifically proved for their taste.



Yet, despite these reservations, most participants felt that they had experienced a free form of thinking unhindered by rational barriers. For many, this shift started as they had to imagine the mythical creatures. Participants told this was the point where they started to stop thinking about the goal and the meaning of the exercise and just started to draw and write whatever came up, without worrying about the results. Some told that they had previously worked with other methods designed to stimulate “outside-the-box” thinking, they noted that these methods still imposed restrictions related to the purpose its feasibility and reality of the design. In contrast, the Creator-Destroyer method allowed them to think creatively without restrictions. Or as one of the participants phrased it, about the moment where they got the second assignment and had to draw the mythical creatures: “At that point I thought: WHATEVER! It doesn’t make sense anyway, so I might as well let go of everything.”

Still, what struck us in the reactions afterwards the most was that in many cases, although the method had widened the perspective and given insights, participants were doubtful if this was a very effective method as it felt for them too unrealistic, some even phrasing it as not academic or scientific enough. It seemed as if in their minds something that is not goal oriented and rationally approached, has less value in research. It brings us back to the issue of non-rationality and the challenge of addressing the unknown-unknowns.

### ***Unknown-unknown and non-rationality***

The use of worldbuilding through imagination, drawing and creation led designers to not only broaden their

perspective on their research subject and its stakeholders, but also to recognize how their usual methods had limited their creativity. Immersing themselves into a non-realistic, non-rational world, gave the participating designers a sense of freedom of thinking without boundaries. Even though, thinking as broad as possible is often part of design methods these designers, participants felt that the rational objective of these methods seemed to have caused them to narrow their views. At the same time the non-rational approach of the Creator-Destroyer method had confused them while doing it, as it seemed to miss a purposeful useful direction.

This insight shows a key limitation of current approaches of (design) research methods. They are practical and rational but have as downside that the non-rational aspects of being human are seen as non-scientific and not useful. As a result, these aspects and their possible effects are bound to be overlooked and missed. This suggests that critical unknown-unknowns possibly could be uncovered, if we find ways to integrate methodical thinking with a sense of irrational purposelessness that allows designers to think more freely.

While there are methods to uncover part of the unknown-unknowns, such as Devil's Advocacy and Red Teaming, but they are grounded in reason. They rationally try to uncover the unknowns. These methods try to discover threats by logic and reasoning. This leads us to unknown-knowns (the things we do not know we know) and known-unknowns (the things we know we do not know) and only the part of the unknown-unknowns (the things we do not know, we do not know) that are based

upon realistic rational reasoning. The larger part of the unknown-unknowns is out of the reach of our rational knowledge as we cannot reason them. To access more of these unknown unknowns that remain uncovered we could introduce irrationality into research methods to explore the unknown, this would lead to the following (Ir)rational Knowledge Matrix:

<p><b>Rational Knowns</b></p> <p>What we reason we know</p>	<p><b>Rational Unknowns</b></p> <p>What we reason we do not know</p>
<p><b>Irrational Knowns</b></p> <p>What we know to be irrational but relevant</p>	<p><b>Irrational Unknowns</b></p> <p>The things that are out of reach of rational thinking</p>

### The (Ir)rational Knowledge Matrix

By bringing irrationality in design methods, we could uncover a larger part of the unknown-unknown and add a freedom of thinking that seems to have gotten lost in rational thinking. Our dependence on the powers of reason are not enough to prevent the dangers we do see coming, as Jean-Pierre Dupuy suggests, they leave us defenceless against a headlong rush into the abyss of global warming, nuclear holocaust, and the other catastrophes that loom on our horizon (Dupuy, 2013).

The Creator-Destroyer method provides a structured way to gradually lead participants out of their normal modes of thinking into playful mode. The method guides participants through a series of steps, helping them immerse themselves in a different world with different rules. The objective is to turn the participants into malignant mythical creatures, participants are encouraged to explore how their (security) designs could be perverted, to make life miserable or in the case of a security design, the security could be breached in unexpected ways.

### ***Conclusions***

This article focuses on a way of red teaming that addresses two key challenges:

- Conducting red teaming without relying on external people, while remaining fresh perspectives;
- Overcoming the rationality bias in the thinking of most professionals.

The Creator-Destroyer method tackles both issues. Tested in the Netherlands, the exercise is designed to detach the security officers from their daily routine and thinking – by inventing and playing a mythical persona, with mythical powers, that pose a threat for the interests they are tasked protecting. The rationality bias is addressed by tapping into the deeper level of archetypes and non-rationality.

By bringing non-rationality into design methods, we can uncover a larger part of the unknown- unknown and add a freedom of thinking that seems to have gotten lost in rational thinking. In doing so, the residual threat of the

unknown-unknowns is further reduced – and more threats can be identified.

Participants reflections revealed that letting go of rationality and the way they were normally accustomed to doing design research, was what holding these designers back in thinking free about possibilities and dangers. All the methods they were accustomed were aimed at making the (security) design better, whether it be through understanding the users, the context, or the working itself. For many, a design method had to be useful in the sense that it would be aimed at the intended use and would generate purposeful outcomes, that could be implemented in the design on a practical way. At the same time almost all participants acknowledged that the method allowed them think more freely about possibilities than any other method they had used before.

Although thinking as broad as possible is always part of design methods these practitioners used, they felt that the rational, goal-oriented nature of their methods had unintentionally narrowed their view. This was the most valuable insight from the Creator-Destroyer exercises. Part of the unknown-unknown harmful effects of a design could be uncovered if we find ways to integrate methodical thinking with a sense of irrational purposelessness. This realization led to the final iteration of the Creator-Destroyer method, which promotes the use of non-rationality in design methods. The goal is to give non-rationality a place in methodical design research – including security design – so that it becomes more widely accepted. In doing so, we open the possibilities for discovering more of the unknown-unknowns.

## Literature

1. Amnesty International. (2022). *The social atrocity: Meta and the right to remedy for the Rohingya*. London: Amnesty International.
2. Berkowitz, L. (2008). On the consideration of automatic as well as controlled psychological processes in aggression. *Aggressive Behavior: Official Journal of the International Society for Research on Aggression*, 34(2), 117-129.
3. Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach for evaluating risk of targeted violence. *Behavioral Sciences & the Law*, 17(3), 323-337.
4. Bridle, J. (2018). *The new dark age: Technology and the end of the future*. London: Verso Books.
5. Buenfeld, G. (2020). *The botanical mind*. London: Camden Art Centre.
6. Cooper, A. (1995). *About face: The essentials of user interface design*. Indianapolis: IDG Books.
7. DeLong, T. W. (1970). *A fault tree manual research report: Presented in partial fulfillment of the requirements for the degree Master of Engineering*. Industrial Engineering. Department of Texas A&M University.
8. Department of the Army, Headquarters. (1959). *Field Manual 30-101: Aggressor the maneuver enemy*. USA: Department of the Army.
9. Dupuy, J.-P. (2013). *The mark of the sacred*. Stanford, CA: Stanford University Press.
10. De Valk, G. (2018). 'Critical Infrastructure and the Unknown: a Methodological Quest'. *National Security and the Future*, 19(1-2).
11. De Valk, G., & Goldbach, O. (2020). "Towards a robust  $\beta$  research design: On reasoning and different classes of unknowns". *Journal of Intelligence History*, 20(1), 72–87.
12. De Valk, G. (2023). 'Total Warning'. *National Security and the Future*, 24(3).
13. Gibbs, G. (1988). *Learning by doing: A guide to teaching and learning methods*. Oxford: Oxford Polytechnic.
14. Gray, D., Brown, S., & Macanujo, J. (2010). *Game storming: A playbook for innovators, rulebreakers, and changemakers*. Sebastopol, CA: O'Reilly Media.

15. Habermas, J. (2011). *Myth and ritual*. Cambridge: Polity Press.
16. Hall, Hill. (2019). Meaning-making, suffering, and religion: a worldview conception. 22(5), 467–479. APA PsycInfo. <https://doi.org/10.1080/13674676.2019.1625037>
17. Huizinga, J. (1938). *Homo ludens: A study of the play-element in culture*. London: Routledge & Kegan Paul.
18. Jung, C. G. (1951). *Aion: Phenomenology of the self*. Princeton, NJ: Princeton University Press.
19. Jung, C. G. (1953). *Collected Works of CG Jung, Volume 9 (Part 2): Aion Researches into the Phenomenology of the Self (Vol. 9)*. Princeton University Press.
20. Luft, J., & Ingham, H. (1955). *The Johari window: A graphic model of interpersonal awareness*. Los Angeles: University of California Press.
21. Malik, K. (2002). *Man, beast, and zombie: What science can and cannot tell us about human nature*. London: Weidenfeld & Nicolson.
22. Mathieu, C. (2017). *Identity and masked rituals*. Academia.edu. [www.academia.edu/34771018/Identity\\_and\\_Masked\\_Rituals](http://www.academia.edu/34771018/Identity_and_Masked_Rituals)
23. Musharbash, Y. (2018). *Monsters*. Sydney: Sydney University Press.
24. Proliferation Resistance and Physical Protection Evaluation Methodology Working Group. (2009). *PR&PP evaluation: ESFR full system case study final report*.
25. Stackelberg, Mc Dowell, (2015) 'What in the World? Storyworlds, Science Fiction, and Futures Studies'. *Journal of Futures Studies*, 20(2): 25–46.
26. Taleb, N. N. (2007). *The black swan: The impact of the highly improbable*. New York: Random House.
27. Tangherlini, T. R. (2018). *Toward a generative model of legend: Pizzas, bridges, vaccines, and witches*. *Journal of American Folklore*, 131(521), 377-399.
28. University of Foreign Military and Cultural Studies, TRADOC G-2 Intelligence Support Activity. (2018). *The Red Team Handbook (version 9.0)*. Chapter 7.
29. USA. (2004). *The Intelligence Reform and Terrorism Prevention Act of 2004 (Title I of Public Law 108-458; 118 Stat. 3688; Sec. 2005, System Assessments, (d)(2)(A))*.

30. Van der Plas, L., & Leeuwenkamp, W. (2018). Pro-actief beveiligen en predictive profiling. Utrecht: KSI.

All images by Djie Han Thung.