Global Governance Futures

ROBERT BOSCH FOUNDATION
MULTILATERAL DIALOGUES

The Future of Weaponized Unmanned Systems: Challenges and Opportunities

TAKAAKI ASANO
ABDULRAHMAN EL-SAYED
KRYSTLE KAUL
KEVIN KÖRNER
WEI LIU
SWATI MALIK
MIO NOZOE

MAY 2015

Supported by

Robert Bosch Stiftung

GGF Partners

GPPi GLOBAL PUBLIC POLICY INSTITUTE
The Tokyo Foundation 東京財団
BROOKINGS
Hertie School of Governance
Keio University
ASHOKA UNIVERSITY
WOODROW WILSON SCHOOL

Acronyms

CCW	United Nations Convention on Certain Conventional Weapons
DMZ	Demilitarized Zone
DN	DefenseNet
GPS	Global Positioning System
ICRAC	International Committee for Robot Arms Control
ISIS	Islamic State in Iraq and Syria
LeT	Lashkar-e-Taiba (Pakistan)
MTCR	Missile Technology Control Regime
PLA	People's Liberation Army (China)
R&D	Research and Development
RUWUST	Restricted Use of Weaponized Unmanned Systems Treaty
SP-10	Security Power-10
UAVs	Unmanned Aerial Vehicles
UNSC	United Nations Security Council
WUAVs	Weaponized Unmanned Aerial Vehicles
WUS	Weaponized Unmanned Systems
WUSVs	Weaponized Unmanned Submerged Vehicles

Cover photo: US Air Force Photo / Lt. Col. Leslie Pratt

Table of Contents

About the Program

The Global Governance Futures program (GGF) brings together young professionals to look ahead 10 years and to recommend ways to address global challenges.

Building on the success of the first two rounds of the program (GGF 2020 and GGF 2022), GGF 2025 assembled 25 GGF fellows from Germany, China, Japan, India and the United States (five from each country). Over the course of 2014 and 2015, the fellows participated in four dialogue sessions: in Berlin (8-12 June 2014), Tokyo and Beijing (9-15 October 2014), New Delhi (18-22 January 2015) and Washington, DC (3-7 May 2015).

The GGF 2025 fellows – a diverse mix from the public, private and non-profit sectors, and selected from a highly competitive field of applicants – formed three working groups that focused on Internet governance, geoengineering governance and global arms control, respectively. Using instruments from the field of futures research, the working groups produced scenarios for their respective issue areas. These scenarios are potential histories, not predictions, of the future. Based on their findings, the fellows produced a range of publications – including this report – that present recommendations for steps to take on these issues towards a more desirable future.

The greatest asset of the program is the diversity of the fellows and the collective energy they develop when they discuss, debate and engage with each other during the four intense working sessions. This is why the fellows occupy the center stage of the program, setting GGF apart from many other young-leaders programs. The fellows play an active role in shaping the agenda of their working groups. The working process draws upon the GGF method and brings together the unique strengths, experiences and perspectives of each fellow in working towards a

common goal. In addition, the fellows meet with leading policymakers and experts from each participating country. The GGF team works closely with the fellows to help them achieve their goals and, in the process, cultivates a community that will last well beyond the duration of the program, through a growing and active alumni network.

GGF is made possible by a broad array of dedicated supporters. The program was initiated by the Global Public Policy Institute (GPPi), along with the Robert Bosch Stiftung. The program consortium is composed of academic institutions, foundations and think tanks from across the five participating countries. The GGF partners are GPPi, the Hertie School of Governance, Tsinghua University, Fudan University, Ashoka University, the Centre for Policy Research, the Tokyo Foundation, Keio University, the Woodrow Wilson School of Public and International Affairs, and the Brookings Institution. The core responsibility for the design and implementation of the program lies with the GGF program team at GPPi. In addition, GGF relies on the advice and guidance of the GGF steering committee, made up of senior policymakers and academics. The program is generously supported by the Robert Bosch Stiftung.

The fellows of the global arms control working group would like to thank the organizers of GGF 2025, the Robert Bosch Stiftung and everyone else who contributed to making the program possible – especially Thorsten Benner, Michelle Chang, Mirko Hohmann, Johannes Gabriel and Joel Sandhu. We are also grateful to Alex Fragstein for the design work, Oliver Read and Esther Yi for editing and colleagues at GPPi for commenting on this report.

Executive Summary

In recent years, challenges concerning the use of weaponized unmanned systems (WUS)[1] – airborne, seaborne or on the ground – have taken the world stage in political and military planning efforts. This trend will continue over the next decade, as these weapon systems have inevitable implications for security and defense strategy among major international actors and smaller actors alike. Addressing the challenges to global security and stability will require determined action by national actors, non-governmental organizations and intergovernmental organizations.

This report presents two hypothetical scenarios and argues that the state of international peace by the year 2025 will depend largely on whether state and non-state actors are capable of designing an effective political and legal framework for regulating the use of WUS without infringing on their profound commercial capabilities.

In the first scenario, WUS exist as linchpins in both the expanded war on terror and conventional interstate conflicts. The scenario highlights that weaponized unmanned aerial vehicles (WUAVs) are likely to continue playing a role in military efforts against global jihadi terrorism, with a growing degree of autonomy. These technologies also feature prominently in important regional conflicts. Against this backdrop, technical failures of WUS – such as hacking and spoofing by terrorists and rogue states – pose a significant threat to safety and security. There exist regional efforts to establish international legislation, but they are thwarted by dominant powers that, in their expanded efforts to combat terrorism on foreign soil, are reliant on WUS. In this scenario, an effective global legal regime on WUS is unlikely to come into being by 2025.

In contrast, our second scenario features an emerging international legal order. The driving force of this development is the perception of a common threat to major actors that possess WUS technology. Here, the threat of international terrorism extends beyond the United States and other Western countries, to Russia and China. In this scenario, terrorist exploitation of weaknesses in these systems in Europe and Asia creates the political context for stricter regulation. In addition, this scenario considers private-sector interests. The dual-use aspect of unmanned systems, especially unmanned aerial vehicles (UAVs), is represented by a thriving

commercial UAV industry, transforming logistics and transportation. Private-sector resistance to regulation that could obstruct market potential is counterbalanced by government incentives to prevent the weaponization of small-scale commercial UAVs. This scenario concludes with the establishment of a workable international regime on WUS, wherein governments agree to regulate the most-advanced systems with the highest degree of autonomy, which only a few countries possess as of 2025.

Several policy recommendations arise from these scenarios:

› Propose a legal framework to govern the production, accumulation, distribution and use of semi-autonomous WUS and to ban fully autonomous WUS;
› Diversify the policy conversation across the continuum of applications of unmanned vehicles;
› Create a policy forum to establish dialogue about applicable standards;
› Seek political-power balance, and seize opportunities for agreement;
› Address technical challenges posed by unmanned systems.

[1] *Weaponized unmanned systems (WUS) include vehicles, robotics and equipment that have the capability to inflict harm upon individuals and/or damage to infrastructure (eg, weaponized unmanned aerial vehicles [WUAVs]). These systems can be either semi-autonomous or fully autonomous.*

Introduction

The idea of launching a surprise strategic attack on a moving vehicle from 10,000 miles away by using a remote-controlled unmanned aerial vehicle (UAV) would have seemed far-fetched two decades ago. But this concept has been fully realized today. The forms of weaponized unmanned systems (WUS) and the degree of their use in international conflicts have increased in the last decade. In tandem, a variety of relevant logistical, ethical, legal and strategic questions have arisen.

Particularly concerning is the potential rise of autonomous WUS with the capacity to search and destroy targets without requiring human control or authorization. While no such systems exist today, technical research aimed at achieving autonomy has intensified. Furthermore, simple forms of autonomous weapon systems – including active protection systems for ground vehicles – already exist, and several major powers are actively funding the development of systems, such as the US's X-47B unmanned combat air system, China's Lijian ("Sharp Sword") and Russia's Mikoyan Skat. The US, the world's most dominant power and WUS user, has articulated its intention to increase the autonomous capacity of its systems.[2]

Autonomous WUS pose several challenges, including the potential for hacking and spoofing, increased casualties, faulty or unstable machine learning that leads to erratic behavior, and the engagement of autonomous systems with human systems or other autonomous systems, resulting in unintended consequences. Furthermore, they pose important questions. Who bears responsibility in the case that an autonomous weapon causes casualties? How susceptible are these weapons to hacking and spoofing? How will governments react to provocations resulting from these systems?

While technical research into autonomous WUS is progressing, there has been little development regarding these ethico-legal implications, and no international agreement on how best to approach the impending age of autonomy. As recently as November 2014, states in the United Nations Convention on Certain Conventional Weapons (CCW) discussed the need for deliberations on lethal autonomous weapon systems that raise critical issues of legal and ethical consideration. As such, demands to ban the development, production and use of autonomous weapon systems have become more resolute. Representatives of many countries have made strong cases for a guarantee of "meaningful human control" to guide the use of such weapons, which suggests that support is growing.

Nevertheless, several challenges to this approach remain. First, there are commercial uses for many of the technologies that could be leveraged towards the development of autonomous WUS, making regulation a challenge. Second, heavy military investment in the development of autonomous weapons technology has been, for the most part, driven by the fight against global jihadi terrorism, the threat of which continues to grow. These challenges may limit the willingness of governments and corporations to suppress their investments.

Through a rigorous process, we identified the main drivers of WUS governance and developed two complementary but contrasting scenarios for the evolution of WUS and their governance over the next 10 years. Upon developing these

[2] *Lt. Gen. Dave Deptula, "Air Force Unmanned Aerial System (UAS) Flight Plan 2009-2047" (Headquarters US Air Force, May 2009), available <http://www.defense.gov/dodcmsshare/briefingslide/339/090723-D-6570C-001.pdf> (accessed 16 March 2015).*

scenarios, contrasting them and deducing operative opportunities and threats from each, we isolated key policy recommendations for promoting stability in the future.

Timeline of Events for Scenarios 1 and 2

YEARS	SCENARIO 1	SCENARIO 2
2015–2017	› China-Japan tensions rise, following the discovery of oil in the East China Sea and increased political and economic pressures in both countries. Efforts to establish a bilateral crisis-management mechanism fail. › North Korea is allegedly running a WUS research program, according to US intelligence. › In 2016, a coalition of Peshmerga and Shiite forces, coupled with US airstrikes, defeats the Islamic State of Iraq and Syria (ISIS), but its leader, Abu Bakr al-Baghdadi, manages to escape. › In 2016, US and EU begin development of DefenseNet, a semi-autonomous unmanned weapon system based on advanced machine learning.	› Starting 2015, the UAV market sees dramatic growth. › In October 2016, a sea-pirate group hacks a Chinese WUSV and uses the systems to attack China's offshore rig in the South China Sea. › In February 2017, an Islamist militant group spoofs a Russian WUAV and tries to sell it on the black market. › In May 2017, a small-scale commercial UAV carrying an explosive crashes into the French socialist party's headquarters, injuring several people.
2018–2019	› In 2018, Baghdadi founds a new global terror network, called al-Majma'a, following the demise of ISIS. › In 2019, several serious terrorist attacks, including in London and Washington, DC, further strengthen the US/EU fight against al-Majma'a. › Starting 2019, Japan and China inject substantial funding into the development and promotion of drone technology and infrastructure, in response to the East China Sea conflict.	› In 2018, the UAV industry develops, and creates more than 2 million jobs. › In September 2018, Lashkar-e-Taiba (LeT) crashes a WUAV into the US embassy in Islamabad, killing several Pakistanis and Americans, including the US ambassador. › In January 2019, at the World Economic Forum in Davos, world leaders establish a working group under the Missile Technology Control Regime to discuss WUS issues and propose a definition of WUS. › In March 2019, the US-LeT conflict escalates. The US assassinates LeT's leader, and LeT commits to retaliation. › Public pressure to regulate WUS rises in South Asia, Europe and US. › Throughout 2019, business leaders and high-ranking representatives from EU, US and Israel meet regularly to negotiate the regulation of fully autonomous WUS. › In December 2019, the San Francisco Protocol is issued to limit the use of commercial UAVs. › Due to rising pressure, US and other major WUS-producing countries agree to two-year moratorium on the production and use of fully autonomous WUS.

YEARS	SCENARIO 1	SCENARIO 2
2020–2021	› In April 2020, China's People's Liberation Army loses communication with one of its WUAVs on a surveillance mission. The WUAV, using topographical recognition memory, charts back to China but intrudes on Japanese airspace along the way. › China-Japan relations hit rock bottom, and the countries come close to war. India, Australia and South Korea mediate China-Japan tensions in consultation with US. › In 2020, DefenseNet goes live (the next year, it becomes fully operational), significantly curtailing the expansion of al-Majma'a. › Attempts to formalize an international treaty regime on unmanned systems, led by India, fail due to fierce opposition from US and UK, given their counterterrorism operations.	› Economies of China and Russia decline. › In May 2020, major states and non-state actors gather in Geneva to discuss LeT attacks and how they might be prevented in the future. › In August 2020, Brazil, China, France, Germany, India, Israel, Japan, Russia, UK and US formally sign a two-year moratorium, banning the use of fully autonomous WUS. › In fall 2021, France, UK and US table a draft resolution about WUS control to the UN Security Council (UNSC). China and Russia, still recovering from economic downturn, decide not to abstain.
2022–2023	› In 2023, a South Korean surveillance drone goes missing. North Korea claims successful spoofing and landing of a drone in North Korean territory, but this is disputed by US intelligence. › The counterterrorism success of DefenseNet is clouded over by repeated erratic behavior and faulty targeting in friendly airspace. › By 2023, al-Majma'a has expanded its influence and acquired a global force of over 100,000 combatants.	› In May 2022, the UNSC adopts a code of conduct to ban fully autonomous WUS for those who had disposed of these systems and to make them unavailable for those who sought to acquire it. › In October 2022, US convenes a conference of all countries possessing sophisticated WUS technology to discuss a possible international treaty on the regulation of fully autonomous WUS.
2024–2025	› The unprecedented rise in drone-related incidents leads to the establishment of the International Weaponized Robotics Control Statement of Intent, led by China, Japan and India, and supported by many other nations. The statement draws substantial criticism from US and EU.	› In June 2024, states sign the Restricted Use of Weaponized Unmanned Systems Treaty (RUWUST) and, based on the treaty, form the regulative body Security Power-10. › In December 2025, RUWUST officially takes effect.

CRUCIAL FACTOR	FACTOR OUTCOME IN SCENARIO 1	FACTOR OUTCOME IN SCENARIO 2
Weapons technology	Development and deployment of WUS with humans "out of the loop"	Maintenance of WUS with humans "on the loop"
Terrorism (state and non-state actors)	Influence of terrorism increases	Influence of terrorism declines
Non-state actors (nonviolent)	Non-state actors grow in the political sphere of influence	Non-state actors gain international recognition
Hacking and hijacking	Capacity to hack/hijack WUS grows at pace with security mechanisms to protect WUS against misuse	Security mechanisms develop faster than the capacity to hack/hijack WUS, allowing military forces to operate without outside interference
Leadership	Influence and power of rogue leaders increase	Influence and power of rogue leaders decrease
Codification of ethics and norms	Global fracture prevents the codification of norms and the formulation of enforceable treaties	Codification of emergent norms leads to the formulation of enforceable treaties
Enforceability	Enforceability is certain	Enforceability is certain
Casualties, and errant use of WUS	Geopolitcal influence of casualties and errant use decrease	Geopolitcal influence of casualties and errant use decrease
Distribution of WUS	WUS are unevenly distributed among major powers	WUS are evenly distributed among major powers
Domestic security	Social unrest, terrorism and crime increase; trust in public and political institutions is low	Social unrest, terrorism and crime remain at usual levels; trust in public and political institutions is high
Foreign policy	Global order is fractured, and states are more willing to act unilaterally	States prefer to achieve their foreign-policy objectives through consensus
Defense budget	Defense budget for WUS R&D and production increases	Defense budget for WUS R&D and production increases
Commercial interests	Semi- and fully autonomous WUS technologies are developed and not constrained	Semi- and fully autonomous WUS technologies are developed but constrained
Cost of war	Cost of war continues to increase	Cost of war continues to increase
Sovereignty	Concept of Westphalian sovereignty, as reflected by actions of states, declines	Concept of Westphalian sovereignty, as reflected by actions of states, is strengthened

Scenario 1: Weaponized Unmanned Systems in a Fractured World

By 2025, there has been a significant rise in the development of unmanned vehicle systems. At the same time, China and India have emerged as major foci of global financial investment and economic growth. China's rapid rise is accompanied by increasing regional instability, particularly in the East China Sea.

The escalation of hostility between emergent China and Japan over the Senkaku/Diaoyu Islands, where oil has been found, brought the two countries to the brink of war. This occurred after a drone of the Chinese People's Liberation Army (PLA) lost contact with ground control during a routine flight over the islands. The PLA drone had been preprogrammed to chart the shortest distance back to the mainland using topographical recognition memory, causing it to enter disputed airspace that was de facto under Japan's control, in the East China Sea. The drone was subsequently downed in the disputed airspace by a Japanese scramble mission. The Chinese government interpreted this as an act of aggression, heightening tension in the region. India, along with the international community, tried hard to deescalate tensions and to facilitate negotiations to prevent the crisis from worsening.

Further agitating the region was North Korea's spoofing[3] of a South Korean drone in 2023. North Korea claimed that it successfully landed the drone in its territory. However, the Ministry of Defense in Seoul and the United States intelligence community claimed that the vehicle had not successfully landed, but rather crashed in the Korean Demilitarized Zone (DMZ).

These events united the region against the threat of weaponized unmanned systems (WUS). China, Japan and India led the formulation of the International Weaponized Robotics Statement of Intent to limit the use of WUS, which has been a major focus of the United Nations

[3] *Spoofing is when a person or program successfully masquerades as another by broadcasting falsified data.*

Convention on Certain Conventional Weapons. The statement has drawn substantial criticism from the US and the European Union, which argue that it "empowers the terrorists" by limiting the types of weapons that can be used against them.

The reason for this resistance is that by 2018, al-Majma'a ("the Coalition") – a global terror network created following the demise of the Islamic State in Iraq and Syria (ISIS) – established itself as the most powerful and influential terrorist organization. It recruits heavily from disaffected young men in the Middle East, South Asia and Europe, and has a global force of over 100,000 combatants. In addition, it has formed coalitions with like-minded groups in Nigeria, Pakistan and Afghanistan, helping to create a global terror network. The stated aim of al-Majma'a is to establish an Islamic caliphate under the strictest interpretation of Sharia law, to establish dominance in the Middle East and to "uproot the evils of Western imperialism."

In Iraq and Syria, it has seized control of pockets of territory ranging from the Golan Heights to Mosul, and has conducted attacks in the US and several European cities, including a major bomb attack on the Capitol building in Washington, DC, resulting in 37 deaths. Although beleaguered and withering, the governments of Iraq and Syria have been able to rely on support from the EU and the US, which have propped up local dictators in the region.

The war against al-Majma'a is driven by investments from Western powers (namely, EU member states and the US), in the form of traditional ground war as well as in the development of DefenseNet (DN), which began in 2016. DN is an autonomous weapon system that relies on advanced machine-learning technologies to target, hunt and destroy al-Majma'a cells. Although DN requires human authorization to execute its attacks, it combines the use of human intelligence with advanced visual, audio and infrared sensor technologies to deliver accurate information regarding the likelihood that a target – whether human or infrastructural – belongs to al-Majma'a forces. Weaponry ranges from Predator-3 unmanned aerial vehicles to larger bombers like the B-2020, which carry advanced warheads, such as the HypeWar, as well as smaller, 500-centimeter UAVs equipped with precision bombs for surgical strikes.

While these efforts have effectively curtailed the growth of al-Majma'a since 2023, the erratic behavior of several DN unmanned weapons is concerning. A number of weapons have gone missing over the past two years.

How We Got Here

The Senkaku/Diaoyu Islands in the East China Sea have been a hot spot for the past several years. China has been claiming discovery and ownership of the islands since the 14th century, and Japan controlled the islands from 1895 to 1945. Both countries have invested in weaponized robotics throughout their territorial disputes. Since 2019, China has built 11 drone bases along its eastern coast and conducted several flight tests near the islands with combat drones equipped with stealth technology. At the same time, Japan's Ministry of Defense has contracted Northrop Grumman, one of the world's largest UAV manufacturers, to produce maritime versions of the Global Hawk (a UAV surveillance aircraft) to identify and track foreign ships and UAVs, with the goal of deterring the Chinese threat.

Following several near-incidents in which Chinese drones, including weaponized unmanned aerial vehicles (WUAVs), briefly entered Japanese airspace around the Senkaku/Diaoyu Islands, Japan warned that it would

down foreign vehicles violating what it considers its airspace. In response, China declared that any attack on its fleet would be considered an act of aggression and be redressed. An unexpectedly difficult economic recession and public unrest in China led to a further rise in Chinese nationalism as an instrument of social cohesion. Domestic pressures also translated into a felt necessity for Chinese officials to stand strong in territorial disputes, while Japan's foreign policy apparatus was dominated by the imperative to save face on the regional stage. Efforts to establish a maritime and aerial crisis-management mechanism between the two countries repeatedly failed as tension grew in the East China Sea.

During a thunderstorm in April 2020, the PLA lost communication with one of its WUAVs on a surveillance mission around the islands. In accordance with emergency protocol in the case of lost connection to Global Positioning System (GPS) navigation, the WUAV used topographical recognition memory to chart the shortest route back to its Chinese coastal airbase, thereby intruding into Japan-controlled airspace around the disputed islands. A Japanese scramble mission was deployed in response. After the Japanese pilot's failed attempts to communicate with and land the drone through radio contact and signaling, the drone was shot down over the disputed territories as a display of will. With communication between Beijing and Tokyo grinding to a halt, the situation escalated, and both sides deployed substantial navy and air-force contingents to the area.

The unfolding crisis alerted the international community to the immediate possibility of war. In talks mediated by India, Australia and South Korea, and with the US's consultation, China and Japan were brought back to the negotiating table, and further escalation of the situation was averted. Upon the urging of Indian, Australian and South Korean mediators, as well as the US, both countries agreed upon the urgent need to install standing mechanisms for crisis communication and management, as well as the need for a common understanding regarding the use of unmanned vehicles in conflicts.

In 2023, a South Korean surveillance drone that had been deployed at the North Korean border went missing. There were conflicting reports regarding its whereabouts. However, such a situation was not unprecedented: three small UAVs with digital cameras had been detected at the Korean border by South Korea's Ministry of National Defense as early as 2014, and other unmanned and unarmed aircrafts had also been found in different locations in South Korea over the previous nine years. Although North Korea never released any official comments about these incidents, US intelligence reports indicated that North Korea had been developing weaponized robotics and had contracted an Iranian expert for research on weaponized robotics technology. North Korea claimed that the drone had been spoofed and successfully landed in North Korean territory, while the Ministry of Defense in Seoul and the US intelligence community claimed that the drone crashed in the Korean DMZ and never landed successfully.

Collectively, these events have had a profound impact on Asian geopolitics. The events have reoriented the region's attention to rivalries between states that are now armed with WUAVs. India, with the support of Australia and South Korea, led the mediation. Although India may seem like an unusual partner, its growing economic power and political influence – resulting in part from growing discussions regarding its potential as a new member of the UN Security Council (UNSC) – has made its government more confident about leading the mediation process. And given that an all-out conflict would, on balance, have severe repercussions for the economies of all three countries, China and Japan were less hesitant to accept India's role. This, along with back-door discussions facilitated by Australia between China, India and the US, convinced China to set aside its past differences with India and to allow India to take on the role of arbitrator in the regional dispute.

Empowered by this role, and in an effort to avoid similar challenges in the future, India led in 2025 the formulation of the International Weaponized Robotics Statement of Intent, with tacit support from China and Japan. The statement, which has

been a major focus of the UN Convention on Certain Conventional Weapons, limits the use of large weaponized systems and reinforces the need for direct human control of all aspects of these systems. The statement has drawn substantial criticism from the US and the EU, which argue that it "empowers the terrorists" by limiting the types of weapons that can be used against them. Prior to the formulation of the Statement of Intent, there had been forceful attempts by many nations – including India, Brazil and Russia – to advocate for a treaty regime on unmanned systems that focuses on fully autonomous weapon systems that remove humans from direct control of system actions. In fact, a draft specimen of the legislation had been circulated among the experts present at a related meeting of the CCW in 2020. However, all attempts to formalize such a legal structure were thwarted by the US and the United Kingdom, both of which aggressively dismissed the regulation bid.

Meanwhile, in the Middle East, a coalition of Peshmerga and Shiite forces, coupled with US airstrikes, defeated ISIS in 2016, although its leader, Abu Bakr al-Baghdadi, disappeared before he could be captured. In 2017, his name began to reemerge in intelligence reports out of Iraq. Within a year, his new organization, al-Majma'a ("the Coalition"), cemented its role as a marquee global terrorist organization, with former ISIS militants, Boko Haram, the Taliban, al-Qaeda and others joining under its banner. Recruitment from the Middle East, North Africa, South Asia and particularly Europe continued to intensify. By 2023, the size of the organization's global movement reached an estimated 100,000 combatants, including men and women.

In a spate of terrorist attacks between 2018 and 2020, al-Majma'a and its allies attacked a number of targets in Germany, the UK and the US. Although American and European forces had been conducting targeted strikes against key strongholds in Iraq and Syria, a coordinated attack on The Gherkin in London and the Capitol building in Washington, DC, on 11 September 2019 killed 359 people combined and galvanized anti-al-Majma'a sentiment. In 2020, the US and the EU committed several thousand ground troops to fight al-Majma'a forces. In addition, they launched a previously experimental program, DefenseNet. Designed by the same team that created Israel's Iron Dome missile-defense system, DN employs a semi-autonomous weapon system that combines on-the-ground human intelligence with advanced visual, audio and infrared sensor technologies to identify and destroy al-Majma'a targets in Syria and Iraq, with DN bases throughout the Middle East, in Egypt, Saudi Arabia, the United Arab Emirates and Kuwait.

These Middle Eastern countries continue to commit to the fight by providing both troops and financial support. In addition, Nouri al-Maliki has resumed power of the ailing Iraqi government, and North American and European support for the Bashar al-Assad regime in Syria and the Maliki regime in Iraq persists, although the value of these relationships remains unclear. While Assad and Maliki have served as important alternative governments to ISIS (and now al-Majma'a) in their respective countries, their forces have been implicated in a number of atrocities, causing over 500,000 casualties across the region since 2015.

DN has effectively curtailed the growth of al-Majma'a since 2020. Al-Majma'a has sustained heavy casualties from DN attacks and has lost several high-profile battles. However, DN has not been without its own challenges from the beginning. After becoming fully operational in 2021, there were several reports of erratic behavior, with the system being forced to power down on several occasions due to "faulty targeting": several DN drones were intercepted in friendly airspace while they were about to carry out attacks. Despite these limitations, the US and the EU assured their interlocutors that they had "fixed the bugs," and that DN was safe, effective and the greatest anti-terrorism weapon in history. Furthermore, domestic support for these programs continues in the US and the EU, following several al-Majma'a attacks on targets in both regions. For this reason, the US and the EU have denounced the India-sponsored Statement of Intent, arguing that it will empower the terrorists and that such regulation would further destabilize the Middle East.

Opportunities and Threats

This scenario contains a number of threats and opportunities that influence how the future plays out. First, the potential technical liabilities of WUS are important threats that shape two different incidents in the scenario. In the first incident, North Korea leverages technical liabilities to spoof a weaponized drone: falsified GPS data is fed into the drone's system after its GPS connection has been jammed. In the second incident, a Chinese People's Liberation Army weaponized drone loses contact with ground control and subsequently follows an automated protocol, using topographical recognition memory to chart the shortest distance back to its origin. The drone flies into disputed airspace and triggers a diplomatic crisis between China and Japan. Hence, spoofing – and inadequate technical protections or protocols in its aftermath – is an important threat that emerges from this scenario.

The second threat is the lack of consensus among powerful state actors regarding the importance of regulating WUS and the resulting global imbalance in global security influence. With the spoofing of drone technology and the subsequent loss of contact between the drone and its command center, technical challenges have destabilized Asian geopolitics. Given what is at stake for Asian powers, China, India and Japan have been galvanized to fight the threats posed by the errant use of WUS. As a result, they have come together to draft the International Weaponized Robotics Statement of Intent, which reinforces the need for direct human control of all aspects of these systems. However, political realities differ substantially between the US and the EU, which are embroiled in a decades-long war against terrorist networks in the Middle East. For this reason, the US and the UK have threatened to block any efforts to regulate the use of WUS, which, they argue, empower terrorists. Moreover, given their position on the UN Security Council, this opposition threatens the viability of any regulation.

The third threat is that both non-state actors and rogue states continue to hold power. While we recognize that the threat posed by these actors may not directly impact WUS governance, such actors play an important role in shaping the trajectory of the first scenario. Both al-Majma'a and North Korea are engaged in destabilizing Asian geopolitics, as well as geopolitics between the Middle East and the West. In that respect, they pose a uniquely important threat that can manipulate other threats like technical liabilities and global power inequities, such as those between the US and the UK, and between the Asian powers.

An important opportunity arising from our scenario is the codification of norms and the creation of law regarding the regulation of WUS. Although there remains global disagreement on the import of such regulation in our scenario (and any meaningful regulation on WUS use may require time beyond 2025), the establishment of the International Weaponized Robotics Statement of Intent in this scenario suggests that regional agreement on the issue may be an important step towards meaningful regulation. In particular, beyond the obvious regulatory implications of limiting autonomous WUS, the conversations required to establish such regulation have the potential to lead to an enhanced global understanding of the opportunities and threats associated with these systems.

Scenario 2: Weaponized Unmanned Systems in a New World Order

From 2015 to 2025, the world has witnessed a rapid development in unmanned vehicle technology – such as unmanned aerial, sea and ground vehicles – in both civilian and military sectors. A significant increase in computational resources, combined with cloud computing and breakthroughs in sensor technology, has led to a new generation of small-scale unmanned aerial vehicles (UAVs) for commercial use in various industries. The same technological advances have also spawned new types of large-scale weaponized unmanned systems (WUS) for military use, causing a paradigmatic shift in the composition of armed forces worldwide, as well as in military strategic thinking.

During this same period, the threat of terrorism has dramatically escalated, with a series of attacks around the world targeting civilians, state officials and critical infrastructure. Major incidents that took place in China, Europe, Pakistan and Russia displayed similar characteristics despite their geographic variation: the use of weaponized unmanned aerial vehicles (WUAVs) to commit acts of terrorism. Beginning early 2015, terrorist perpetrators undertook a strategic shift towards the use of UAVs in order to disrupt domestic security at the highest possible levels. A series of terrorist attacks between 2015 and 2018 illustrated the global significance of the threat of WUS falling into the wrong hands.

CHINA: In October 2016, a sea-pirate group saw an opportune moment and hacked into one of China's newly developed weaponized unmanned submerged vehicles (WUSVs), Haiyan, after news quickly spread that it was experiencing technical difficulties and that its security system was vulnerable. The pirates then used

Haiyan to launch a small-scale attack on an offshore Chinese rig in the South China Sea. The rig was constructed and jointly owned by Shell and China's third-largest national oil company, the China National Offshore Oil Corporation. The attack resulted in three casualties and three missing persons, including a Dutch and an American, who were both engineers. China, the Netherlands and the US condemned the terrorist group and initiated a joint search for the missing persons. This incident, along with the extensive search, attracted widespread international media coverage.

RUSSIA: In February 2017, Vilayat Dagestan, an Islamist militant group, took control of a Russian WUAV that was being tested in the Dagestan province. The group gained control primarily by spoofing. Vilayat Dagestan managed to land the WUAV at a terrorist safe house in Chechnya. It then publicized the capture and offered to sell the airframe and surveillance equipment to any black-market buyer. Prior to this incident, Russia had been trying to develop a national drone program, partnering with the Chinese on defense technology.

FRANCE: In May 2017, following a series of events in which commercial UAVs violated the airspace over nuclear power plants and government buildings in France in late 2014 and early 2015, a small-scale commercial UAV carrying an explosive crashed into the French socialist party's headquarters. This incident occurred shortly after President François Hollande's re-election. Several people were severely injured. A small French militant right-wing group later claimed responsibility for the attack, which was intended to protest the socialist government's stance on immigration.

US AND PAKISTAN: In September 2018, Lashkar-e-Taiba (LeT), a Pakistani terrorist organization, took control of a fully autonomous American WUAV patrolling Pakistani airspace in North Waziristan and redirected its flight course to Islamabad. The group gained control of the WUAV and redirected it by jamming – that is, crowding and then blocking – the GPS signal so that the WUAV was made to believe that it was following its preprogrammed GPS coordinates, when in reality it was following substituted coordinates. LeT crashed the WUAV into the US embassy in Islamabad, killing six Pakistanis and 13 American officials, including the US ambassador. The group immediately claimed responsibility for the incident. Official reports later confirmed that LeT was able not only to broadcast a fake GPS signal, but also to shut off the transponder and to program new GPS coordinates, targeting the US embassy. In doing so, LeT operatives were capable of taking the WUAV off the radar and sending it to its target in a short amount of time, leaving little time for the Americans to react. As a direct consequence, the US dramatically escalated its drone strikes throughout Pakistan's Waziristan region and the North-West Frontier Province in an effort to wipe out LeT's terrorist network and other similar groups. The US managed to kill LeT's leader in March 2019. The next day, LeT's new leader threatened to target US interests in retaliation.

The political consequences of the September 2018 attack dealt a severe blow to US-Pakistan relations and strengthened the US "war on terror." As a direct result of the hijacking of the fully autonomous WUAV, there was global uproar about the use of such systems. A larger group of UN member states, human rights groups and other civil-society actors pointed fingers at Israel and the US for producing dangerous technology that could fall so easily into the hands of terrorist hackers.

How We Got Here

In light of these incidents, governments around the world began to invest heavily in anti-jamming and anti-spoofing technologies to prevent further attacks like those that occurred in China, Pakistan and Russia. Larger jammers were set up in the vicinity of critical infrastructure around the world to cut off communication between UAVs and their ground control, hence making any UAV – even the smallest, commercially available types – non-operational within a certain perimeter.

In the aftermath of the incidents, there was heightened international debate on whether the predominantly unregulated arena of WUS technology should fall under tighter legal control. Given the urgency of the situation, world leaders present at the World Economic Forum in Davos, Switzerland in January 2019 decided to set up a working group under the Missile Technology Control Regime (MTCR)[4] to discuss WUS issues.

In trying to determine the definition of WUS, the MTCR relied extensively on external expertise provided by the International Committee for Robot Arms Control (ICRAC), a non-governmental organization comprised of international experts on robotic arms. This special body served as a critical link between the political-legal and the technological dimensions of the WUS issue.

Soon thereafter, however, the challenges of creating legally binding regulations came to the fore. The market volume for commercially used UAVs doubled per annum between 2015 and 2018, creating thriving new industries and services in China, Europe and the US. It was estimated that more than 2 million jobs were created in this sector on a global scale between 2018 and 2019.

At the 2019 World Economic Forum, governments announced their effort to agree on a common definition of WUS as a basis for a more regulatory approach, which incited concern from representatives of their respective commercial industries. As a result of the incessant lobbying efforts in the capitals of major stakeholders, the commercial WUS industry managed to limit government interference in its daily activities. Policymakers needed to strike a delicate balance between making the world more resilient against the abuse of unmanned systems, and avoiding the prevention of fledgling industries from growing and creating jobs and revenue. Throughout 2019, business leaders and high-ranking representatives from the EU, Israel and the US met regularly to agree on a deal calling for greater oversight and control of the commercial use of WUS. Governments agreed to limit the technological development of fully autonomous WUS. At the same time, they asked for guarantees from companies to implement measures that increase security in all facilities and to provide regular reports about the production of such weapons. After 10 months of continuous negotiations, the EU, Israel and the US adopted a non-legally binding WUS Memorandum of Understanding to increase transparency about technological innovation, to allow greater government oversight and restrictions on WUS production and to share any concerns about the hackability of WUS. This gentlemen's agreement held significant political importance for the players involved and built a sense of trust.

Global public antagonism towards fully autonomous WUS was running high, with NGOs and other civil-society groups fearing that fully autonomous WUS would take a life of their own and move out of human control. States felt the need to respond to the growing resentment

[4] *The MTCR is an informal and voluntary partnership between more than 30 countries to prevent the proliferation of missile and UAV technology that is capable of carrying a 500-kilogram payload for at least 300 kilometers.*

against the technology. Finally, in December 2019, the San Francisco Protocol emerged. Major commercial UAV companies accepted the request of international governments, expressed through the MTCR, that WUS technology develop simultaneously with the technology to control it. In addition, UAV companies made the guarantee that WUAVs would not operate close to critical infrastructure. Companies expressed their commitment to ensuring significant funding for research and development (R&D) aimed at finding technological solutions, to prevent WUS from entering special areas of concern (eg, power plants, the water supply, telecommunications, government institutions). Additionally, companies agreed to provide anti-WUS technology like anti-jammers to government institutions only.

Governments felt more comfortable with the San Francisco Protocol in place because they were reassured that commercial companies building unmanned systems would not have access to technological know-how and critical infrastructure for possibly weaponizing their systems. Hence, one of the greatest challenges faced by the MTCR during the early stages of its work was to draw a clear line between commercial and military uses of unmanned systems. With the San Francisco Protocol in place, the attention of world leaders shifted in subsequent years to addressing the growing concern of powerful interest groups about fully autonomous WUS.

In light of the incidents in Europe, China, Russia and elsewhere – in particular the attack in Pakistan – all of the major powers that possessed sophisticated WUS, along with the members of the UN Security Council, the state parties to the CCW, the International Atomic Energy Agency, the MTCR and key non-state actors like ICRAC, gathered for the first time in May 2020 in Geneva to discuss the attacks and preventive measures for the future. The outcome of the first Geneva meeting was minimal. No document was drafted, and no political declaration was published. However, relevant state actors decided to reconvene four times a year.

Meanwhile, throughout 2019, the year following the Pakistan incident, anti-American protests in Islamabad, Lahore and Karachi intensified due to the misuse of a fully autonomous WUAV, wherein the GPS signal was jammed and then redirected to hit the US embassy in Pakistan. Protests also spread across the Western world, resulting from the civilian perception and fear of a future in which fully automated warfare is inevitable. The question of how much autonomy should be given to machines, especially in the area of modern warfare, captured public attention in the West and gradually developed from a mere technical issue into a crucial political question. Rising civilian pressure, along with the political ramifications of US President Hillary Clinton's attempt to secure votes for re-election in the 2020 presidential race, triggered a dialogue with other major WUS-producing countries that led to consensus on a two-year moratorium on the production and use of fully autonomous WUS.

During this period, no fully autonomous WUS was to be put into operation while new security mechanisms to protect such systems from outside interference (eg, hacking) were being tested. The moratorium did not apply to other types of WUS (where a human is involved in the machine's decision-making) and civilian UAV production (as it is already governed by the San Francisco Protocol). Israel agreed to President Clinton's initiative in return for unofficial US support for a new settlement plan in Palestine's West Bank.

China and Russia, each maintaining considerable and costly research programs on WUS, demonstrated little willingness to accept any measure that would halt these programs. Yet, as a result of a downward economic spiral in both countries in the early 2020s, Beijing and Moscow finally agreed to the moratorium as part of cost-cutting efforts in their military sectors. Their rationale went as follows: if they were no longer able to invest in WUS programs as much as before, to reduce the technological gap with the US, then their best option was to make sure that the US would not make any further technological advances in this particular field. In addition, China's and Russia's WUS research was

primarily driven by state-owned companies, whereas the US's R&D of WUS was run entirely by private-sector companies. Thus, a moratorium could have had a significant effect on US industries in this market, which might have proved less resilient than their heavily subsidized state-owned counterparts.

In August 2020, Brazil, China, France, Germany, India, Israel, Japan, Russia, the UK and the US signed a two-year standstill agreement banning the use of fully autonomous WUS. In consequence, the lead private defense contractors, such as Lockheed Martin and Northrop Grumman, suffered great financial losses as the US military decreased the number of private contracts to produce fully autonomous WUS (which, at that time, dominated the defense market), given the US's new policy to restrict the use of, and reduce spending on, fully autonomous WUS. However, the number of contracts to enhance firewalls increased because of a strong need to prevent the hacking and jamming of GPS signals. In light of those business aspects, the standstill agreement brought about a short-lived reduction of public revolt against fully autonomous WUS in Europe and the US. Widespread discontent soon resurfaced, as major NGOs and interest groups sought a permanent extension of the moratorium, beyond 2022.

During the EU-US summit in fall 2021, both sides agreed to call for an international code of conduct[5] regulating the development, production and deployment of fully autonomous WUS. In a joint initiative, France, the UK and the US tabled a draft resolution at the UNSC. China and Russia, still recovering from an economic downturn, decided not to abstain. The two countries also realized that the technology gap with the US could only be closed at a high cost. Therefore, the second-best solution was to ban this technology for those who had disposed of it, and to make it unavailable for those who sought to acquire it. As such, the code of conduct was adopted in May 2022.

Seizing the opportunity to set aside decades of skepticism towards international treaties (including in the area of arms control) and to silence its critics, the US convened in October 2022 a conference of all countries possessing sophisticated WUS technology to discuss a possible international treaty on the regulation of fully autonomous WUS. After more than a year of intense negotiations, the countries drafted the Restricted Use of Weaponized Unmanned Systems Treaty (RUWUST), an international legal framework banning fully autonomous weapon systems. The RUWUST also created a council called the Security Power-10 (SP-10), composed of the major WUS-producing states: Brazil, China, France, Germany, India, Israel, Japan, Russia, the UK and the US.

By 1 June 2024, the RUWUST signatory states reached an agreement that featured the following: (1) a standard for semi-autonomous weaponized unmanned vehicles and a ban on fully autonomous WUS were agreed upon for the first time in history, (2) a RUWUST inspection and verification body was installed, and member states agreed to periodic inspections of all WUS facilities, (3) countries agreed to share information about their WUS programs, and (4) countries would work together to prevent the proliferation of fully autonomous WUS technology to third parties. The treaty banned the use of fully autonomous WUS, with a provision that the ban could be lifted after the two-year moratorium period, so long as there was a unanimous vote within the SP-10 Council to do so.

Signatory countries agreed to meet regularly in order to follow up on the implementation of the treaty and to stay up to date with changing technology and developments on the ground. Upon a series of follow-up conferences, signatory states signed an agreement on 19 December 2025 to ban all fully autonomous WUS. The rationale behind the decision was the notion that militaries do not want to relinquish control of weapons, and

[5] *This international code of conduct was an agreed-upon set of norms, according to which member states restrict their use of WUS. Additionally, these states agreed to establish sophisticated security systems to prevent violent non-state actors from acquiring WUS, and agreed to institute a protocol wherein the state handles any WUS-hacking incidents with the help of member states, the UNSC, the CCW and ICRAC.*

that risks surrounding the errant use of WUS were far too high. Hence, states agreed that semi-autonomous WUS can be just as lethal as fully autonomous WUS, but involve more oversight and checks and balances to minimize the potential for error and collateral damage. All member states agreed to cooperate with RUWUST's SP-10 Council in the event that a violent non-state actor operating within a state conducts a WUS attack. SP-10 Council members would determine at what point to intervene in a state, when an internal, violent non-state actor kills a significant number of individuals or causes significant damage to infrastructure, and when state authorities are manifestly failing to stop this type of violence. This process is reviewed on a case-by-case basis in conjunction with the International Coalition for the Responsibility to Protect.

With respect to the treaty, signatory nations are less inclined to breach the principles of RUWUST because the political, economic, social and security consequences are extremely high, especially in a globalized world where states are interdependent and reliant on commercial and weapons trade. The states are deterred from using WUS against each other because of the notion of reciprocity, wherein if one nation strikes, there may be direct retaliation. Therefore, an imperfect balance of power is created, in which states decide to ban fully autonomous WUS in an effort to maintain a strong level of human oversight.

Opportunities and Threats

Several opportunities and threats for global arms control emerge from our second scenario. First, the San Francisco Protocol and RUWUST both demonstrate the potential for the mobilization of the international community to respond to unexpected attacks involving smaller commercial UAVs or large-scale WUS. Violent attacks and incidents described in this scenario attract the media's attention, create intergovernmental dialogue and can potentially create a global movement by civil society groups to limit the use of such weaponized systems. It is debatable whether progress in the legal codification of international norms governing the use of WUS would be possible in the rather short time span of 10 years without such incidents taking place.

Second, the opportunity to leverage cross-regional disputes towards global support is a main point. No national actor – be it China, Russia or the US – can be entirely certain about operating its WUS fleet without the risk of it falling into the hands of unauthorized users. The incidents between 2015 and 2018, as described in this scenario, emphasize the global scale of the challenge. The fact that no major player in the area of WUS is able to secure and shield its systems against external interference eventually leads to a common perception of threats linked to WUS. A common-threat perception is a suitable starting point for intergovernmental dialogue, leading to a commonly agreed-upon definition and ultimately an effective codification of norms. Regardless of differences in the global outlook and the foreign policies of China, Russia and the US, there is considerable potential for cooperation in the WUS arena, as none of the three powers has the assurance that it will be spared by the need to address the security of its own WUS, either regionally or globally. In turn, this kind of enhanced cooperation might lead to a spill-over effect into other conflict areas and encourage dialogue and agreement on controversial issues outside of the WUS context.

Another important threat against drone technology is jamming, spoofing and hacking. The same technological progress that brought about the ever-increasing sophistication of WUS will also lead to their ever-growing insecurity. The rise of computing power and the ubiquity of inexpensive, commercial UAV supplies, combined with the spread of expertise in the field of WUS around the globe, could significantly increase the likelihood of such weapon systems becoming prone to external security threats. As with many other closed-circuit computer systems, the technological means to gain unauthorized access to such systems could evolve one step ahead of countermeasures to protect them. Recent incidents of hacking – eg, the US Central Command website, databases at Sony Pictures and critical infrastructure with Stuxnet – appears to confirm this tendency. Given that all computer networks have some potential vulnerabilities (in other words, they are "hackable"), the likelihood of a malignant non-state actor trying to penetrate a network is higher because he or she can go undetected and subsequently cause severe damage.

The final and most critical threat is global terrorism, especially international jihadism, which is unlikely to decrease in intensity between now and the year 2025, posing another threat in our scenario to both the governance of WUS and the implications for international security. Specifically, RUWUST holds states accountable for preventing violent non-state actors from acquiring WUS. Al-Qaeda has been rivaled by both the media and newer terrorist organizations such as Boko Haram, al-Shabab and ISIS. These new factions pursue a strategy entirely different from that of conventional jihadist groups. Instead of exclusively capitalizing on shocking terror attacks at home and abroad, they use terrorist methods to gain control of a defined territory in failing or war-torn states. In doing so, they often replace the traditional state order, thereby creating safe havens and training grounds for a new generation of terrorists. With local governments unable to regain control of some of these territories, and with the international community reluctant to pay the political price for full-scale intervention (eg, boots on the ground), these terrorist groups have created sanctuaries. Such sanctuaries allow them to attract a more diversified crowd of followers, including skilled computer experts, some of whom hold degrees from renowned academic institutions. The highly sophisticated propaganda used by ISIS to lure disenfranchised Western youth into global jihad is a telling example of the increasing technical expertise of such groups. This sophistication coupled with spoofing magnifies the threat of both.

Policy Recommendations

Propose a legal framework such as the Restricted Use of Weaponized Unmanned Systems Treaty to govern the production, accumulation, distribution and use of semi-autonomous WUS and to completely ban fully autonomous WUS.

Expediting the process of establishing an associated legal framework is an important unifying goal while weaponized unmanned systems (WUS) are still in the early stages of evolution. One way forward involves enacting new laws that address areas of concern regarding WUS, as well as declaring the relevance and applicability of appropriate existing laws. This might ensure that the designers and users of military WUS develop and utilize their technology in ways that conform to legal standards. Such an international legal framework, when combined with domestic state norms and best practices, would significantly help the regulation of WUS.

Diversify the policy conversation across the continuum of applications of unmanned vehicles, in both academic and policy forums.

While commercial discourse about the application of unmanned technologies has grown more nuanced, public and policy discussions on the opportunities and threats of different types of technologies have remained relatively blunt. In that respect, rather than having one discussion about "drones," thought leaders and policy centers should push for a more diverse set of conversations, stratifying conversations by weaponizability, automation, size, range and intended use. In this respect, small drones that might deliver our groceries need to be differentiated from large drones equipped with Hellfire missiles.

Such a stratified discourse will have three advantages: First, and most importantly, it is more likely to avoid overregulation, which could limit the positive benefits of commercial use. Second, a more nuanced policy conversation is more likely to attract allies in the private sector, who would be less fearful of regulation. Third, the specificity of the discourse has the potential to increase the likelihood of meaningful regulation of large and increasingly automated weaponized robotics, unencumbered by the fear of potential overregulation.

Create a policy forum that unites leaders from key corporations, academics, and government and military representatives under the auspices of the UN Convention on Certain Conventional Weapons or other intragovernmental organizations to establish a dialogue about applicable standards that can maximize commercial development of these technologies while minimizing the potential for harm.

Decisions on the nature of laws, the specificity of their provisions and the frequency of revisions must first be preceded by constructive dialogue at the international and domestic levels. One of the first steps towards meaningful legislation is to establish shared definitions of categories or thresholds of autonomy (ie, formalize definitions of terms like "fully autonomous" and "semi-autonomous") and types of technology, which would likely prove to be a contentious and protracted process, as countries will struggle to find consensus. Furthermore, a joint understanding of the principle of "meaningful human control" vis-à-vis WUS is required to facilitate the development and enforceability of

new international laws. Second, in determining the legality of weapon systems, international humanitarian law and human rights law will need particular examination. Third, to provide for questions of accountability, such a framework should include specific standards of liability for any unexpected consequences arising from the use of WUS, including casualties, collateral damage and unintended conflict, for the producers of WUS as well as the commanders that authorize their use.

In addition, there need to be well-defined and mutually agreed-upon standards of care for all parties involved in the manufacturing, use and transfer of such technology. Also in need of enunciation are details of the liability actions that could be brought about in case of related omissions. The process of introducing a legal regime to govern the use, production, accumulation and distribution of WUS will no doubt be full of challenges, yet a regulatory framework is the only way to mitigate the potential harms and to maximize the advantages of WUS.

Seek political-power balance, and seize opportunities for agreement.

A primary challenge across our scenarios is the imbalance of power and its threat to global security. While militarily powerful countries that possess weapons, like the UK and the US, may have the most to lose in the case of regulation, the less powerful have-nots may have the most to lose in the case of continued deployment. The reality remains that even powerful states are deterred by the notion of retaliation and are less likely to launch WUS against another major WUS state, which leads to an imperfect balance of power. In that respect, achieving balance should be a primary goal in efforts to mitigate the threats posed by WUS.

While the reorganization of key power structures (eg, the UN Security Council) may be instrumental in increasing representation, it is beyond the scope of our recommendations. But there are several softer means of balancing influence on these issues. First, organizations with multilateral representation and both intellectual and political authority on these issues – such as the International Committee for Robot Arms Control and the UN Committee on Disarmament – should be further empowered to convene global discussions and to set the discursive and regulatory agenda regarding the use of WUS. Second, these organizations should be opportunistic, taking advantage of key events to convene broader conversations about the threats and opportunities posed by WUS. Third, internationally recognized bodies that could provide expertise and influence public opinion on the human cost of WUS use, such as the International Committee of the Red Cross (the custodian of international humanitarian law), should be further engaged by governments interested in regulation.

Address technical challenges posed by unmanned systems.

Unmanned systems for civilian and particularly military purposes increasingly pose important challenges: first, the lack of available tracking and control systems, and second, the threat of spoofing, jamming and hacking of unmanned systems by terrorists, criminals and rogue states. To address the first challenge, major funding and effort should be allocated to research and development of adequate tracking and registration technologies for unmanned aerial vehicles in order to mitigate security and accident risks. Also, global institutional frameworks should provide guidelines for required technologies and regulation. This may include the creation of an international registration system for unmanned vehicles and a licensing protocol for pilots, akin to that for automobiles and manned aviation. Similarly, protocols should be adopted to systematize UAV air-traffic control communication. Automatic no-fly zones (eg, around airports, nuclear power plants, government buildings, military installations, hospitals, schools) should be required for all commercial UAVs.

To mitigate risks of hijacking and misuse of unmanned vehicle systems, strict national and international certification requirements regarding such systems' security technology

should be set for developers. Given the global development and distribution of unmanned vehicles technology, the security standards of national aviation/traffic regulators should be harmonized internationally – through, for example, organizations like the International Civil Aviation Organization, the UN Economic Commission for Europe, and the World Forum for Harmonization of Vehicle Regulations. Similarly, research and development of anti-spoofing and anti-hacking technologies are needed, and international funding for research into these technologies could be one way forward. Potential areas of focus could include reducing reliance on GPS technology and improving communication-encryption technologies.

Fellows of the Global Arms Control Working Group

TAKAAKI ASANO is a research fellow at the Tokyo Foundation. His general area of expertise is Japanese foreign and national security policy and international trade policy. Previously, he was a policy research manager at the Japan Association of Corporate Executives (JACE, or Keizai Doyukai), an influential business organization in Japan, where he was responsible for JACE's international programs and edited various policy proposals. Prior to joining JACE, he was the senior research analyst at the Representative Office of the Development Bank of Japan in Washington, DC, where he authored policy reports on a wide range of issues, from politics to financial and economic policy. He earned his bachelor's in sociology from the University of Tokyo, and received his master's in international relations from New York University.

ABDULRAHMAN EL-SAYED is an assistant professor in the Department of Epidemiology at Columbia University, where his research considers how our social realities make us sick. He has authored over 50 peer-reviewed scientific articles, commentaries and book chapters, and has been featured at national and international conferences. He is also a fellow at Demos, a non-partisan public policy center. His commentaries have been featured in The New York Times, CNN, Al Jazeera, Project Syndicate, The Guardian and Huffington Post. He regularly raises debates on health policy, with a particular focus on disease prevention in light of health trends. He is also a regular commentator on public health and medical issues at Al Jazeera America. He earned a PhD in population health from Oxford University as a Rhodes Scholar, and an MD from Columbia University as a Soros Fellow and Medical Scientist Training Program Fellow. He received his bachelor's in biology and political science from the University of Michigan with Highest Distinction.

KRYSTLE KAUL is a senior consultant in the Federal Practice at Deloitte Consulting LLP, where she primarily works with the US Department of Defense. She is also a briefing instructor at Linktank and a participant in the Department of Homeland Security's 2015 Intelligence Community-Private Sector Analyst Program. Prior to Deloitte, Krystle worked for Leidos as a political-military analyst at the US Department of Defense, monitoring security issues in the Middle East. Before joining Leidos, Krystle was an adjunct staff member at RAND Corporation, spearheading a study on Afghanistan's civil-military operations centers. Additionally, she gained experience managing projects funded by

the US Agency for International Development at Chemonics International, assisting with Haitian disaster relief at the American Red Cross, writing health and education reports for UN Women and researching national security issues on Capitol Hill. Her think tank experience includes the Carnegie Endowment for International Peace, the Woodrow Wilson International Center for Scholars and the Center for Strategic and International Studies. Her research examines nonviolent and violent protests within the Kashmiri and Palestinian national movements. She has also been awarded a number of grants to participate in delegations to India, Israel, Bosnia and Herzegovina, Cyprus and Greece. Krystle holds a bachelor's in international studies from American University's School of International Service, a master's in international relations from Johns Hopkins School of Advanced International Studies and a master's in political science from Brown University, where she has been pursuing her PhD.

KEVIN KÖRNER is a senior economist and emerging market country risk analyst at Deutsche Bank Research, with a focus on the Middle East and Eastern Europe. He briefs and advises clients both inside and outside of Deutsche Bank on economic and political developments in emerging markets and provides internal country risk ratings. During his research and studies, he developed a particular interest in emerging markets, financial crises and questions related to international security. He frequently publishes on regional topics such as the Arab uprisings, Gulf countries' developments and the EU's eastern expansion. Before joining Deutsche Bank, he completed the European Central Bank's two-year graduate program, working in the economics and communications directorates. Kevin holds a master's in financial economics from Maastricht University and a bachelor's in philosophy and economics from Bayreuth University.

WEI LIU is an assistant professor at the School of Public Administration and Policy at Renmin University of China. Her teaching and research interests include policy processes, international organizations and Chinese politics. She has published many articles on these topics. She also leads the Center of Global Governance at the Academy of Public Policy at Renmin University of China and is in charge of several research projects, including "The Mechanism of Global Public Policy" and "Non-Traditional Security in Southeast Asia." She is actively involved in policy consulting and has been working with several governmental and public agencies like China's State Oceanic Administration and the China Development Bank. Wei is also a visiting professor at the Gerald R. Ford School of Public Policy at the University of Michigan, where she teaches Chinese foreign policy. She holds a PhD in political science from Arizona State University and a master's of law from Peking University.

SWATI MALIK serves as a legal officer at the UN Mission in the Republic of South Sudan. In this capacity, she provides legal advice, research, analysis and drafting support to the mission leadership with a view to facilitating the mission's mandate in South Sudan. Swati specializes in public international law, human rights and public health, and is experienced in Indian and international legal practice. Over the course of her career, she has held positions in diverse jurisdictions, including India, Malaysia and the UK. Prior to joining the UN Department of Peacekeeping Operations, Swati worked at the UN Children's Fund to study an accountability mechanism in the context of children affected by HIV/AIDS, and was also part of the reproductive-rights unit of the Human Rights Law Network, an Indian NGO that was instrumental in securing the first decision in the history of Indian jurisprudence that recognized maternal mortality as a human rights violation and awarded constitutional damages to the victim's family. Swati studied law at the London School of Economics and Political Science and at Symbiosis Law School. She has been awarded a number of grants and scholarships that led to her studying and working for short periods in the Netherlands, Germany, Austria, Italy and Japan.

MIO NOZOE is currently working for the Nutrition Program Unit at the UN World Food Programme (WFP) in Yemen. She is in charge of national mother and child nutrition operations with expertise in government-NGO coordination and project management. As a national of Japan, Mio joined the WFP in 2003 and has served as a program officer in Sri Lanka (including one year with the post-tsunami emergency operation), South Sudan, Somalia and Lao PDR. She also took on short-term emergency coordination positions in post-flood Pakistan and after the 2011 Tohoku earthquake in Japan. She has more than 10 years of experience in complex emergency coordination, post-conflict operations, leading inter-agency partnership, development of action and monitoring plans, donor coordination, NGO partnership, advocacy and information management. She holds a master's in social policy and planning in developing countries from the London School of Economics and Political Science.

Annex: Scenario-Planning Methodology

METHODOLOGY The methodology underlying this report is structured scenario planning. Commonplace at private- and public-sector organizations, the methodology is designed to facilitate strategic long-term planning in the face of an uncertain future. A "scenario" is a possible and internally consistent trajectory of the future. To develop scenarios, the Global Governance Futures 2025 global arms control working group performed four steps: First, we collected and investigated variables that we hypothesized would influence the future of global weaponized unmanned systems (WUS) governance. Second, we performed a factor-system analysis to distill the most crucial factors. Third, drawing upon this analysis, we constructed two scenarios. And fourth, by comparing similarities and differences between these two scenarios, we derived key strategic implications and policy options.

ENVIRONMENT AND FACTOR ANALYSIS We tabulated the most salient technological, social, economic and geopolitical developments that influence the governance of weaponized unmanned systems. These included, among other things, trends related to new weapons technology, domestic security, commercial interests and foreign policy. From a list of approximately 40 factors, we identified 15 that stand out for their potential impact and their level of uncertainty. We subsequently defined at least two possible outcomes for each crucial variable to complete our factor analysis.

FACTOR-SYSTEM ANALYSIS AND SCENARIO CONSTRUCTION To observe cross-impact and interaction effects, we rated cross-impacts between all crucial-factor outcomes and created a matrix of rules for how these factors and their respective outcomes are interrelated. We utilized a computer program (ScenarioWizard) to run a cross-impact balance analysis that separates the plausible and consistent sets of factor outcomes from the inconsistent ones. Then we selected two abstract scenario frameworks. This does not mean that all factors radically differ between the two scenarios. For example, in both scenarios, the hacking or spoofing of WUS plays an important role. But many factors, such as the existence of a consensus legislation, appear only in one scenario. Our scenarios represent two different directions on a continuum of possible futures.

Having defined two plausible and selective future states of WUS governance, we employed a driver-driven analysis to learn more about the forces that primarily influence developments. We then created corresponding histories for our pictures of the future by engaging in a collective writing process. We relied on intra-group discussions and exchanges with experts in the field. We also modeled several development paths for each scenario and engaged in multiple rounds of editing. Recognizing that the future rarely proceeds in a linear fashion, we incorporated turning points into each scenario.

STRATEGIC-IMPLICATIONS FRAMEWORK After they had been outlined and illustrated, the two scenarios underwent extensive plausibility checks during expert reviews. We first accounted for consequences that are "positive" influences (opportunities) or "negative" influences (threats) on arms control governance. Next, we derived strategic options to mitigate threats while utilizing opportunities for each scenario. Third, we determined the strategic fit between both strategy sets and developed a robust lead strategy, including all options that proved to be consistent across both scenarios. This multi-stage process left us with a set of robust strategic options that would be appropriate across scenarios.

As outlined above, we used several techniques – ranging from computerized uncertainty-impact and cross-impact analyses and qualitative content analysis, to input from experts – to make our scenarios robust. In doing so, we profited from many resources:

1. *The interaction of group members who come from a variety of backgrounds, ranging from academia and consultancy, to think tanks and international organizations.* Scenario planning is a holistic approach and requires diversity to tap into different reservoirs of knowledge.
2. *The expertise of our invited experts and speakers.* They made us aware of points of contention that we had overlooked or interaction effects that we had neglected. Thus, they provided not only tacit knowledge but also ample feedback on our descriptors and scenarios.
3. *A rigorous and demanding review process.* We received internal supervision from the GGF team at the Global Public Policy Institute in Berlin, and we benefitted from colleagues who peer-reviewed this report.

This structured scenario approach made it possible for our group to derive targeted and practical options for courses of action in global arms control governance – the governance, specifically, of global weaponized unmanned systems.