Between fragmentation and integration

English summary

ICTs and the popularity of cyber facilities make cyberspace increasingly embedded in the social and economic fabric of societies of the real world. Cybersecurity has become a subject of intense political debates and influences. However, states have distinct or even contradictory understandings on cybersecurity and cyber regulation. Given that contentious matters related to the content and approaches to cybersecurity regulation are deliberated and addressed within the UN framework, and various factions, international collaborations, compromises, and advocacy efforts converge within the UN, it proves valuable to gain a comprehensive and detailed understanding of the advancements, challenges, and potential of global cybersecurity governance at the UN level. Examining and assessing the dynamics of the UN cybersecurity governance is paramount for understanding the prospects of global rules aiming at regulating state conduct and mitigating the impacts of malicious ICTs activities. The main research question of this thesis is: ***To what extent has the UN succeeded in forming global cybersecurity rules, and how can we explain its (lack of) success?***

Chapter 2 introduces concepts, theories, and methods, constructing an analytical framework to address the extent of the UN's achievements in shaping global cybersecurity rules. It establishes a benchmark for success or failure by operationalizing UN rulemaking outcome. Drawing upon Abbott et al.'s concept of legalization, the chapter defines delegation, precision, and obligation as dimensions of outcome. Using existing literature and preliminary empirical findings, the chapter develops indicators to systematically evaluate and comprehend the advancement of rulemaking across the three policy domains in the subsequent empirical chapters. Building upon Yves Schemeil's concept of two scenarios for IOs' growth within a regime complex, which involve cooperation and mutual adjustment at intersections with potential allies and opponents, as well as the management of deliberate processes within the organization's boundaries, the chapter outlines three primary strategies (internal coordination, coalition building, and framing) employed by the UN to promote rulemaking. To understand how the UN engages in cybersecurity regulation and serves a conduit for influencing rulemaking outcomes, the chapter also introduces document analysis. This method aims to explain the factors contributing to the UN's success or lack thereof, considering the perspective of states, international organizations, and policy fields.

Chapter 3 examines the UN's efforts to regulate cyberwarfare. The UN has established professional organs and cooperated with relevant agencies to gain authority in developing cyberwarfare rules, facilitating negotiations and reaching consensus among countries with different perspectives. It has clarified states' responsibilities in cyberspace, covering aspects like sovereignty, non-interference, non-use of force, and due diligence. These efforts emphasize responsible state behavior within the framework of international obligations, however, provide room for interpretation and flexibility in responding to cyber threats. For state behavior standards related to cyberwarfare, the UN thus employs approaches of choosing vague expressions or

selectively omitting contentious elements. The chapter reveals that the UN's achievement in cyberwarfare regulation is characterized by a high level of delegation, medium obligation, and low precision. The chapter also shows that the absence of regular organs hinders the UN's ability to manage negotiations effectively and expand states' consensus. Incompatible interests among major countries and nuanced state blocs undermine rulemaking efforts.

Chapter 4 focuses on UN efforts in cybercrime rulemaking. To address the challenges of regulating cybercrime, the UN has established and coordinated internal organs, acquiring the capability to formulate comprehensive cybercrime rules. Multi-stakeholder participation and capacity building have bolstered the UN's legitimacy in this domain. The UN employs an enumeration approach to criminalization to facilitate consensus, to steer conversations back on the track and to clarify the objectives and scope of cybercrime regulation. The UN has helped reach consensuses on conviction, jurisdiction, and cross-border evidence access, and has established practical activity regulations. The chapter reveals that the UN's accomplishments in cybercrime regulation involves a high level of delegation, medium precision and obligation. The chapter also explains how technical complexity on cybercrime regulation contributes to high delegation but limited precision, and how a Russia-led state bloc amidst conflicts drives the shift towards high delegation. It emphasizes the dominance of states in negotiation and the importance of norm drafting for enhancing precision and obligation.

Chapter 5 examines the UN's efforts to regulate cyberterrorism. To address global counter-cyberterrorism challenges, the UN initiates comprehensive regulation by coordinating its organs. It collaborates with multiple stakeholders, including IOs and private sector representatives, to produce guidelines against cyberterrorism. The UN has also framed cyberterrorism within the context of counterterrorism, which has helped clarify its scope and reduce overlap with cyberattacks and cybercrime. The outcome of the UN regulation in cyberterrorism is marked by a high level of delegation, low precision, and medium obligation. The chapter demonstrates that the ambiguity surrounding the umbrella term "terrorism" makes achieving precision in cyberterrorism rulemaking challenging. It highlights the UN efforts in creating a cohesive and coordinated framework for cyberterrorism governance. However, the absence of a strong drive among states to promote detailed global rules has led to sporadic attention from the UN on this issue.

Chapter 6 compares the processes and results of the UN making rules for cyberwarfare, cybercrime and cyberterrorism. It delves into the disparities in delegation, precision, and obligation within the context of UN activities for cyberwarfare, cybercrime, and cyberterrorism, and provides a summary of the impact of independent variables – power asymmetry, IO resources, and complexity – on the variation observed across these three cases.

The first cluster of variables offering explanations for these rulemaking outcomes pertain to characteristics of the policy field. The technical complexity of an issue area encourages delegation

but tends to hinder precision and obligation. On the one hand, the complexity of cyber issues, with their technological sophistication and legal intricacies, necessitates collaborative international efforts. This creates a demand for states to delegate authority to global bodies. On the other hand, the complexity not only requires the pooling of expertise and resources, but also increases the difficulty of formulating precise rules. Another facet of complexity, political salience restraints obligation. Political salience leads states to prefer retaining their freedom of action and avoiding excessive constraints from international rules. This factor plays a role in elevating the obligation level of cybercrime rules, given its relatively lower political prominence compared to cyberwarfare and cyberterrorism.

Regarding the second cluster of explanatory variables – state relations and power asymmetry between them – the book explores its dynamics within the context of preferences among major powers, state groups, and various actors. The content and homogeneity of preferences determine the rulemaking outcome. Across the three policy domains, a shared objective among major states to regulate cyber issues results in increased delegation to the UN. Conversely, their mutual desire to avoid overly restrictive measures in cyberwarfare and cyberterrorism contributes to lower levels of obligation in these areas. The role of state alliances also becomes evident in shaping the rulemaking outcome. Strong and cohesive state blocs in the realm of cybercrime facilitate elevated delegation, precision, and obligation, whereas in cyberwarfare and cyberterrorism, less cohesive or vulnerable state groups do not exhibit similar effects. Furthermore, the distribution of power between state and non-state actors has an impact on precision. Rule formulation dominated by states in cybercrime yields higher precision, whereas multi-stakeholder involvement in cyberwarfare tends to a lower level of precision.

As to IO resources, the existence of specialized organs and expertise dedicated to specific issues enhances delegation. This exists in all three policy areas. However, the extent of cooperation between these organs influences precision. In cases where there is no single focal organ within a policy field, it tends to hinder precision. In the regulation of cybercrime, a single dominant organ has consistently been maintained, whereas in the regulation of cyberwarfare and cyberterrorism, there are multiple dominant organs. This is also one of the reasons why cybercrime rules stand out in terms of precision compared to the other two domains. It's worth noting that active IO bureaucracy involvement in rulemaking is absent in the areas of cyberwarfare and cyberterrorism. In these domains, staff members primarily focus on research and administrative support rather than taking a lead role in framing discourse or driving negotiation processes to reach consensus. In contrast, while cybercrime regulation exhibits more bureaucratic autonomy, it is constrained by other factors such as staffing levels, preventing cybercrime rules from reaching a high level of precision.

An important finding in this study is the examination of normative discussions within the realm of cybersecurity. It particularly delves into the rivalry among countries globally regarding cybersecurity regulation. This norm contestation in cybersecurity goes beyond the traditional

divide between Western and developing countries and also intersects with the broader context of the competition between the United States and China. The study reveals that, even amid the intense technological competition between the United States and China, the competition over cybersecurity norms in critical ICT areas is not solely influenced by this rivalry. In contrast, China tends to align its positions more closely with those of Russia in shaping the normative landscape of cybersecurity. This underscores the significant role of Russia in influencing the dynamics of norm competition within the global cybersecurity domain.

Nederlandse samenvatting

Informatie-telecommunicatie en de populariteit van cyberfaciliteiten maken cyberspace steeds meer verweven met het sociale en economische weefsel van samenlevingen in de echte wereld. Cybersecurity is een onderwerp geworden van intense politieke debatten en invloeden. Staten hebben echter uiteenlopende, of zelfs tegenstrijdige, opvattingen over cybersecurity en cyberregulering. Aangezien controversiële kwesties met betrekking tot de inhoud en benaderingen van cybersecurityregulering worden besproken en aangepakt binnen het VN-kader, waar verschillende facties, internationale samenwerkingen, compromissen en belangenbehartigingsinspanningen samenkomen, is het waardevol om een uitgebreid en gedetailleerd inzicht te krijgen in de vooruitgang, uitdagingen en mogelijkheden van mondiaal cybersecuritybeheer op VN-niveau. Het onderzoeken en evalueren van de dynamiek van het VN-cybersecuritybeheer is van essentieel belang om inzicht te krijgen in de vooruitzichten op wereldwijde regels die gericht zijn op het reguleren van het gedrag van staten en het beperken van de gevolgen van kwaadaardige ICT-activiteiten. De belangrijkste onderzoeksvraag van deze thesis is: ***In hoeverre is de VN erin geslaagd wereldwijde cybersecurityregels op te stellen, en hoe kunnen we het (gebrek aan) succes daarvan verklaren?***

Hoofdstuk 2 introduceert concepten, theorieën en methoden, en bouwt een analytisch kader om de mate van succes van de VN bij het vormgeven van wereldwijde cybersecurityregels te beoordelen. Het hoofdstuk stelt een maatstaf vast voor succes of falen door de uitkomst van het VN-regelgevingsproces te operationaliseren. Door voort te bouwen op het concept van 'legalisatie' van Abbott et al., definieert het hoofdstuk delegatie, precisie en verplichting als dimensies van de uitkomst. Op basis van bestaande literatuur en voorlopige empirische bevindingen ontwikkelt het hoofdstuk indicatoren om de vooruitgang van het regelgevingsproces in de drie beleidsdomeinen in de daaropvolgende empirische hoofdstukken systematisch te evalueren en te begrijpen. Voortbouwend op Yves Schemeils concept van twee scenario's voor de groei van internationale organisaties binnen een regimecomplex, die samenwerking en onderlinge aanpassing omvatten bij de kruispunten met potentiële bondgenoten en tegenstanders, evenals het beheer van opzettelijke processen binnen de grenzen van de organisatie, schetst het hoofdstuk drie primaire strategieën (interne coördinatie, coalitievorming en framing) die door de VN worden gebruikt om regelvorming te bevorderen. Om te begrijpen hoe de VN betrokken is bij cybersecurityregulering en als een kanaal fungeert voor het beïnvloeden van regelvormingsuitkomsten, introduceert het hoofdstuk ook documentanalyse. Deze methode is bedoeld om de factoren te verklaren die bijdragen aan het succes of gebrek daaraan van de VN, vanuit het perspectief van staten, internationale organisaties en beleidsvelden.

Hoofdstuk 3 onderzoekt de inspanningen van de VN om cyberoorlogsvoering te reguleren. De VN heeft professionele organen opgericht en samengewerkt met relevante agentschappen om autoriteit te verwerven bij het ontwikkelen van cyberoorlogsvoeringsregels, het faciliteren van

onderhandelingen en het bereiken van consensus tussen landen met verschillende perspectieven. De VN heeft de verantwoordelijkheden van staten in cyberspace verduidelijkt, waarbij aspecten als soevereiniteit, non-interventie, niet-gebruik van geweld en zorgplicht aan bod komen. Deze inspanningen benadrukken verantwoordelijk staatsgedrag binnen het kader van internationale verplichtingen, maar bieden ruimte voor interpretatie en flexibiliteit bij het reageren op cyberdreigingen. Voor gedragsnormen van staten met betrekking tot cyberoorlogsvoering hanteert de VN daarom benaderingen waarbij vage uitdrukkingen worden gekozen of selectief controversiële elementen worden weggelaten. Het hoofdstuk onthult dat de prestatie van de VN in de regulering van cyberoorlogsvoering wordt gekenmerkt door een hoog niveau van delegatie, een gemiddelde verplichting en een lage precisie. Het hoofdstuk laat ook zien dat het ontbreken van reguliere organen de VN belemmert bij het effectief beheren van onderhandelingen en het vergroten van de consensus tussen staten. Onverenigbare belangen tussen grote landen en subtiele staatsblokken ondermijnen de inspanningen op het gebied van regelvorming.

Hoofdstuk 4 richt zich op de inspanningen van de VN bij de totstandbrenging van regels voor cybercriminaliteit. Om de uitdagingen van de regulering van cybercriminaliteit aan te pakken, heeft de VN interne organen opgericht en gecoördineerd, waardoor het vermogen is verkregen om uitgebreide cybercriminaliteitsregels op te stellen. Multistakeholderparticipatie en capaciteitsopbouw hebben de legitimiteit van de VN in dit domein versterkt. De VN hanteert een opsommingsbenadering voor criminalisering om consensus te vergemakkelijken, om gesprekken op het juiste spoor te houden en om de doelstellingen en reikwijdte van de regulering van cybercriminaliteit te verduidelijken. De VN heeft geholpen om consensus te bereiken over veroordeling, jurisdictie en grensoverschrijdende toegang tot bewijsmateriaal, en heeft praktische activiteitregelingen vastgesteld. Het hoofdstuk onthult dat de prestaties van de VN bij de regulering van cybercriminaliteit een hoog niveau van delegatie, gemiddelde precisie en verplichting omvatten. Het hoofdstuk verklaart ook hoe technische complexiteit bij de regulering van cybercriminaliteit bijdraagt aan een hoge delegatie maar beperkte precisie, en hoe een door Rusland geleid staatsblok te midden van conflicten de verschuiving naar hoge delegatie aandrijft. Het benadrukt de dominantie van staten in onderhandelingen en het belang van normontwerp voor het verbeteren van precisie en verplichting.

Hoofdstuk 5 onderzoekt de inspanningen van de VN om cyberterrorisme te reguleren. Om wereldwijde uitdagingen op het gebied van cyberterrorisme aan te pakken, initieert de VN een uitgebreide regulering door haar organen te coördineren. Het werkt samen met meerdere belanghebbenden, waaronder internationale organisaties en vertegenwoordigers van de particuliere sector, om richtlijnen tegen cyberterrorisme op te stellen. De VN heeft cyberterrorisme ook gekaderd in de context van terrorismebestrijding, wat heeft geholpen de reikwijdte ervan te verduidelijken en overlap met cyberaanvallen en cybercriminaliteit te verminderen. Het resultaat van de VN-regulering op het gebied van cyberterrorisme wordt gekenmerkt door een hoog niveau van delegatie, lage precisie en een gemiddelde verplichting. Het hoofdstuk laat zien dat de ambiguïteit rond de overkoepelende term “terrorisme” het

moeilijk maakt om precisie te bereiken bij de regelgeving voor cyberterrorisme. Het benadrukt de inspanningen van de VN om een samenhangend en gecoördineerd kader voor cyberterrorismebeheer te creëren. De afwezigheid van een sterke drang onder staten om gedetailleerde mondiale regels te bevorderen, heeft echter geleid tot sporadische aandacht van de VN voor dit onderwerp.

Hoofdstuk 6 vergelijkt de processen en resultaten van de VN bij het opstellen van regels voor cyberoorlogsvoering, cybercriminaliteit en cyberterrorisme. Het verdiept zich in de verschillen in delegatie, precisie en verplichting in de context van VN-activiteiten op het gebied van cyberoorlogsvoering, cybercriminaliteit en cyberterrorisme, en biedt een samenvatting van de impact van onafhankelijke variabelen - machtsasymmetrie, IO-bronnen en complexiteit - op de variatie die in deze drie gevallen wordt waargenomen.

De eerste cluster van variabelen die verklaringen biedt voor deze uitkomsten van regelvorming heeft betrekking op de kenmerken van het beleidsveld. De technische complexiteit van een beleidsgebied bevordert delegatie, maar bemoeilijkt meestal de precisie en verplichting. Enerzijds vereist de complexiteit van cyberkwesties, met hun technologische verfijning en juridische ingewikkeldheid, internationale samenwerking. Dit creëert een vraag naar delegatie van bevoegdheden aan mondiale organen. Anderzijds vergroot deze complexiteit niet alleen de noodzaak om expertise en middelen te bundelen, maar maakt het ook het formuleren van nauwkeurige regels moeilijker. Een ander aspect van complexiteit, politieke urgentie, beperkt de verplichting. Politieke urgentie leidt staten ertoe hun bewegingsvrijheid te behouden en overmatige beperkingen door internationale regels te vermijden. Deze factor speelt een rol bij het verhogen van het verplichtingsniveau van regels voor cybercriminaliteit, gezien het relatief lagere politieke belang in vergelijking met cyberoorlogsvoering en cyberterrorisme.

Wat betreft de tweede cluster van verklarende variabelen – staatsrelaties en machtsasymmetrie daartussen – onderzoekt het boek de dynamiek binnen de context van voorkeuren van grootmachten, staatsgroepen en verschillende actoren. De inhoud en homogeniteit van voorkeuren bepalen het resultaat van de regelgeving. Over de drie beleidsdomeinen heen leidt een gedeeld doel onder de grote staten om cyberkwesties te reguleren tot een verhoogde delegatie naar de VN. Omgekeerd draagt hun wederzijdse wens om te vermijden dat er te beperkende maatregelen worden genomen in cyberoorlogvoering en cyberterrorisme bij aan lagere niveaus van verplichting in deze gebieden. De rol van staatsallianties wordt ook duidelijk in het vormgeven van het resultaat van de regelgeving. Sterke en cohesieve staatsblokken op het gebied van cybercriminaliteit bevorderen verhoogde delegatie, precisie en verplichting, terwijl in cyberoorlogvoering en cyberterrorisme minder cohesieve of kwetsbare staatsgroepen niet dezelfde effecten vertonen. Bovendien heeft de verdeling van macht tussen staat en niet-statelijke actoren invloed op de precisie. Regelgeving gedomineerd door staten in cybercriminaliteit levert een hogere precisie op, terwijl multi-stakeholderbetrokkenheid bij cyberoorlogvoering doorgaans leidt tot een lager niveau van precisie.

Wat betreft de middelen van internationale organisaties, verbetert het bestaan van gespecialiseerde organen en expertise die zijn gewijd aan specifieke kwesties de delegatie. Dit geldt voor alle drie de beleidsgebieden. De mate van samenwerking tussen deze organen beïnvloedt echter de precisie. In gevallen waarin er geen enkel centraal orgaan binnen een beleidsveld is, wordt de precisie vaak belemmerd. Bij de regulering van cybercriminaliteit is er consequent een dominant orgaan gehandhaafd, terwijl er bij de regulering van cyberoorlogsvoering en cyberterrorisme meerdere dominante organen zijn. Dit is ook een van de redenen waarom de regels voor cybercriminaliteit opvallen wat betreft precisie vergeleken met de andere twee domeinen. Het is vermeldenswaard dat actieve betrokkenheid van de bureaucratie van internationale organisaties bij de regelvorming afwezig is in de gebieden van cyberoorlogsvoering en cyberterrorisme. In deze domeinen richten medewerkers zich voornamelijk op onderzoek en administratieve ondersteuning in plaats van een leidende rol te spelen in het vormgeven van discours of het sturen van onderhandelingsprocessen om consensus te bereiken. Daarentegen vertoont de regulering van cybercriminaliteit meer bureaucratische autonomie, maar wordt deze beperkt door andere factoren, zoals personeelsniveaus, wat verhindert dat de regels voor cybercriminaliteit een hoog niveau van precisie bereiken.

Een belangrijke bevinding in deze studie is het onderzoek naar normatieve discussies binnen het domein van cybersecurity. Het richt zich met name op de rivaliteit tussen landen wereldwijd met betrekking tot cybersecurityregulering. Deze normstrijd in cybersecurity gaat verder dan de traditionele scheidslijn tussen westerse en ontwikkelingslanden en kruist ook met de bredere context van de competitie tussen de Verenigde Staten en China. De studie onthult dat, zelfs te midden van de intense technologische concurrentie tussen de Verenigde Staten en China, de concurrentie over cybersecuritynormen in kritieke ICT-gebieden niet uitsluitend door deze rivaliteit wordt beïnvloed. Integendeel, China neigt ertoe zijn standpunten nauwer af te stemmen op die van Rusland bij het vormgeven van het normatieve landschap van cybersecurity. Dit onderstreept de belangrijke rol van Rusland in het beïnvloeden van de dynamiek van normconcurrentie binnen het mondiale cybersecuritydomein.