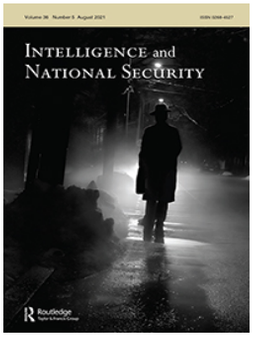

Intelligence and National Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/fint20

Understanding the complexity of intelligence problems

Christiaan Menkveld

To cite this article: Christiaan Menkveld (2021) Understanding the complexity of intelligence problems, Intelligence and National Security, 36:5, 621-641, DOI: 10.1080/02684527.2021.1881865

To link to this article: https://doi.org/10.1080/02684527.2021.1881865

INTELLIGENCE AND NATIONAL SECURITY
2021, VOL. 36, NO. 5, 621–641
https://doi.org/10.1080/02684527.2021.1881865

Routledge
Taylor & Francis Group

ARTICLE

Understanding the complexity of intelligence problems

Christiaan Menkveld

Institute of Security and Global Affairs, Leiden University, The Hague, The Netherlands

ABSTRACT

The complexity of an intelligence problem determines to a great extent the certainty that can be provided by intelligence and security services. This article will argue this deductively and validate this claim using a set of intelligence reports produced by the Dutch Intelligence & Security Service (AIVD). A better understanding of how the level of complexity affects intelligence analysis is helpful for the further (academic) study of analysis methodologies, as well as for managing expectations of intelligence clients, and for informing the debates over legislation that affects intelligence and security services.

Introduction: complexity of intelligence problems

The complexity of an intelligence problem (required intelligence assessment on a certain subject) determines to a great extent the certainty that intelligence and security services can provide on such an assessment. Even though this claim sounds almost obvious, its implications are significant, because it means that the public value of an intelligence service can vary depending on the complexity of an intelligence problem. This ranges from providing 'actionable' intelligence that can lead to interventions (legal, military, interruption operations, etc.), to providing insights that can be used as input for policymakers, and as context for interventions. Therefore, to be effective, intelligence and security services need to take the complexity of an intelligence problem into account when determining the aims of their investigation, the strategy of intelligence collection and its analytic approach. Which also means that intelligence clients and oversight officials and legislators should take the complexity of intelligence problems into account when directing and appraising the performance of services. This article will create a better understanding of this dynamic by describing how the complexity of intelligence problems determines to a great extent the certainty that can be provided by services. Based on this argumentation, the article will finish with some practical insights that can support intelligence and security services, clients, oversight, and legislators to deal with varying levels of complexity per intelligence problem.

Approach

This article will begin with a review of available literature on the complexity of intelligence problems. Then, the concept of complexity will be explained and how it reflects on intelligence problems by combining available literature on complexity and intelligence studies. This will include an overview of features of complex intelligence problems based on a clustering of literature that has listed such features.

CONTACT Christiaan Menkveld s.h.c.menkveld@fgga.leidenuniv.nl

Then, this article will argue deductively how complexity determines to a great extent the certainty that can be provided by services by breaking this claim into individual parts. This will start with a section that will argue how the complexity of an intelligence problem is determined by both the required *type of assessment* and the *subject* of the intelligence problem. For this argument, this article provides an explanation of how the complexity of an intelligence problem can be approximated, as well as a model - based on a combination of available literature and a practitioner's perspective – on how different types of assessments relate to each other. Then in the subsequent section, the concept of a ratio scale for complexity of intelligence problems will be introduced in order to argue that the level of complexity of an intelligence problem determines to a great extent the certainty that can be provided by services. This argument is then validated, based on a study of actual intelligence products of the AIVD.

Finally, the conclusions of this article will be discussed from a practitioner's perspective to identify the practical implications for intelligence and security services, clients, oversight, and legislation.

Literature on the complexity of intelligence problems

This article builds upon available work on 'intelligence problems', 'complex adaptive systems' and the combination of the two.

Intelligence problems are the required assessment on a certain subject. Scientists on intelligence analysis have produced many different categorizations of intelligence assessments, dating back to the early days of Sherman Kent when intelligence analysis became the subject of scientific studies.[1] Some contemporary examples of categorizations include: 'current intelligence vs longer term in-depth analysis, 'positivist vs interpretivist approaches' and 'descriptive, explanatory and 'prognostic research'.[2] There is also some work on the typology of the intelligence problem as a whole, including the 'certain subject' part of the intelligence problem.[3] Vandepeer provides a useful overview of such typologies which includes the widely used 'secrets, puzzles, and mysteries' metaphor and its variations by NATO, Treverton and Ackoff; as well as work by Jones who categorizes intelligence problems in 'simplistic', 'deterministic', 'moderately random', 'severely random' and 'indeterminate'.[4]

'Complex adaptive systems' is a theory that can serve as a paradigm through which one can observe/understand/analyze everything that is 'complex'. It has been applied and researched across scientific domains – ranging from mathematics and biology to social sciences and philosophy – providing a rich body of knowledge that can be applied to all fields. There is also quite some work on the application of complex adaptive systems on the field of international relations, authors like Cederman provide valuable insights on how the theory can practically be applied to analyze 'world politics'. Besides work on complex adaptive systems, there is also academic work from the broader field of complexity studies that provides useful insights on how to apply the concept of complexity in the analysis of social systems like intelligence problems. For example, the book 'system effects' by Jervis shows how dynamics in world politics can be understood in terms of complexity.[5] But also the work of Weaver and consequently Ando et.al. that proves the importance of proper aggregation of variables when analyzing complex social problems and provides tangible guidelines to do so.[6]

There is also a slowly growing body of literature to the application of complex adaptive systems on intelligence analysis, including the identification of 'complexities' as a category of intelligence problems.[7] This is closely related to work on how to organize intelligence collection on complex intelligence problems.[8] However – like most studies on complex adaptive systems – these studies focus primarily on the implications of very complex (intelligence) problems. This article will focus more on how intelligence problems can vary in the level of complexity and the consequences this has on the certainty that can be provided by services. The concepts 'intelligence problem' and 'complex adaptive systems' will be explained in more depth in the upcoming paragraphs using the abovementioned literature.

The concept of complexity

Definition of a complex intelligence problem

An intelligence problem can be considered complex if it aims at:

> 'a network that is adaptive and exhibits aggregate properties that emerge from local interactions among its entities mutually constituting their own environment.'

This definition is based on Cederman's general definition of a complex adaptive system: 'An adaptive network exhibiting aggregate properties that emerge from the local interaction among many agents mutually constituting their own environment'.[9] As you can see the term 'agents' used by Cederman has been replaced with the term 'entities' to avoid confusion with intelligence agents. More importantly, the aspect of 'many' interacting agents/entities has been removed from Cederman's definition, to accommodate varying levels of complexity. There are three aspects of the definition of a complex intelligence problem that require special attention, which will be discussed in line with Cederman's description of his definition, translated to the perspective of intelligence problems.

First: 'The intelligence problem that aims at a network of interacting entities'. As indicated before, an intelligence problem is a required assessment on a certain subject. Every subject that intelligence and security services investigates can be considered a network of entities. Most often such entities will be individuals, but this can also be objects and locations that interact with each other or individuals. For example, a threat assessment of an embassy, which could include the assessment of whether the wall is able to resist an explosion in case the wall would 'interact' with a rocket fired by an attacker. Such a network can also interact with higher aggregated networks that include the individuals working in the embassy and the potential attack planners, as well as the involved governments and terrorist organizations as a whole. Most networks that are part of an intelligence problem will be layered, wherein 'a network subsumes its entities and can itself be part of a larger network'.[10] To what extent interactions between individuals and/or objects are part of the intelligence problem is determined by the required assessment, which delineates the depth and width of the network that is being investigated.

Second: 'Aggregate properties that emerge from interacting entities'. The notion that there are properties that can emerge from interactions, is key to the concept of complexity and why networks of complex intelligence problems are more than just the sum of its entities. For example, the progress of a military campaign is more than just the measurement and comparison of military power of every warring party. It will also likely be the result of the way the military power is used (interaction between parties), how the vehicles are able to cross terrain (interaction between objects), how the command and control structure works (interaction on different levels among warring parties), and many more types of interactions.

Third: 'The network is adaptive and the interactions among entities local'. A network that is adaptive requires at least one entity able to change its interactions based on the outcomes of previous interactions. Such an entity can be any type of 'intelligent being', including bacteria, but it is safe to assume that in most intelligence problems the 'intelligent being' will be human. All of these interacting entities act with limited rationality. Besides the inherent bounded rationality of humans,[11] the rationality of entities in a complex network is also bounded because they depend on 'local' interactions for their observations and (re)actions. The absence of a supreme being that objectively observes all interactions of the network and shares its observations with all entities, means that entities do not have access to all the available information in the network which they require to rationally optimize their actions. For example, a head of state is for its observations dependent on what is 'locally' offered to him/her, this can be intelligence reports, news broadcasts, briefings from advisers, etc. But none of those interactions will be able to provide a complete and objective coverage of what exactly is going on in the country.

Table 1. Clustering of features of complex intelligence problems.

Identified features of complex intelligence problems	Chan	Preiser et.al.	Beebe and Beebe
Nested in environment	Sensitive dependence on initial conditions	Contextually determined	Actors' behavior and the system of interactions that they form can be affected by external or exogenous forces
	Connectivity	Radically open	
Network of interacting entities (first aspect of definition)		Constituted relationally	Often multiple actors, or 'Agents'
Dynamic processes	State of paradox	Dynamic processes	At times, the actors appear to operate on the basis of predictable norms; at other times, they do not
	Far from Equilibrium		The actors can exhibit surprising behavior that cannot be predicted simply by knowing the properties of the actors themselves
Emergence of aggregate properties (second aspect of definition)	Emergent order	Novel qualities emerge through complex causality	
Adaptive based on local interactions (third aspect of definition)		Adaptive capacities	The actors are constantly interacting and adapting in complicated ways
	Distributed control		There is no central controller of the actors' behavior
Path dependency	Co-evolution		Past events can affect actor's behavior
			Actors can choose to adapt their behavior on the basis of their understanding of past events

Features of complex intelligence problems

Complex adaptive systems – like a complex intelligence problem – has some distinct features that are present in any such system. There is a wide array of academic work across scientific fields on identifying and describing such features. In the absence of a unified theory of complex adaptive systems, Chan and Preiser et.al. have listed, clustered and categorized main features that have been identified by leading authors on complex adaptive systems.[12] Specifically on complex intelligence problems, Beebe et.al. have listed some 'hallmarks' that are similar to features of complex adaptive system.[13] By combining the lists by Beebe and Beebe with the frameworks/lists by Preiser et.al. and Chan – see Table 1 – a list of six features inherent to complex intelligence problems has been formulated based on the smallest common denominators. Three of these features equal the three aspects of the complex intelligence problem definition explained in the previous section, the three other features are explained below.

Nested in environment

Complex intelligence problems cannot be fully isolated from their environment. An analyst always needs to take external or exogeneous forces into account regardless of delineation.[14] Delineation is tricky because complex intelligence problems are extremely sensitive to their environment.[15] Very small differences in the (initial) conditions of a complex intelligence problem can lead to radically different results even if the intelligence problem itself is similar. For example, the behavior of two extremist networks guided by the same ideological code operating in two similar countries can act completely differently based on (small) differences in their environment.

Dynamic processes

Complex intelligence problems are inherently nonlinear, meaning that observed effects are not proportional to the magnitude of their causes. The bandwidth of possible outcomes in a complex intelligence problem is very wide.[16] For example, one protester who sets themself on fire does not

make the headline of the local newspaper, whereas another instigates a trans-regional revolution like the 'Arabic Spring'. Furthermore, in complex intelligence problems, there is no single equilibrium but many possible states that are temporarily stable. For example, after protests have started, the trajectory of events can lead to a successful crackdown and the original government still in power, but it can also lead to new stable situations like the installation of a transition government. Such situations are only stable for the time being and have certain tipping points that can be reached by seemingly small events. Knowing that after such tipping point that the trajectory of events will finally lead into a new 'stable' situation that is similar or completely different, is what makes complex intelligence problems very resilient. The space between stability and instability is often referred to as 'the edge of chaos' and is present in any complex intelligence problem, although the frequency wherein transitions between stability and instability occur vary.[17]

Path dependency

Current and future developments in a complex intelligence problem depend heavily on how the individual entities perceive and remember past events, and how this influences their behavior.[18] To continue the previous example, there are many ways that protests can lead to the installation of a transition-government but the future will depend on whether this is the result of years of civil war or that the regime voluntarily stepped down in an early stage. It is important to take into account that the way past events are perceived will vary per entity as they have different abilities, personalities, values, etc. (which by itself are the results of past events). Some will perceive the end of a civil war as victory, others as loss, others who just want violence to end, all of them will likely act differently the next time anti-government protests break out. They will adapt their behaviors based on the way they perceived and remember past events and will respond on the way other entities adapted their behavior, which is called 'co-evolution'.

What determines the complexity of an intelligence problem?

All intelligence problems are complex, but some are more complex than others. The aspects and features mentioned in the previous sections will be present in all intelligence problems with multiple people. However, the extent to which these features occur, and, most important the bandwidth of possibilities that can emerge, depends on how complex an intelligence problem is. In the following section will be explained how the complexity of an intelligence problem can be approximated. Then in the two subsequent sub-paragraphs, this article will argue that the complexity of an intelligence problem is determined by the *type of assessment* and the *nature of the subject*.

Approximation of the complexity of intelligence problems

As the usage of the term 'approximation' already indicates, it is not possible to measure the exact level of complexity of an intelligence problem. However, it will argued that the estimated number of relevant entities combined with the estimated number of their interactions is a practical approximation of the level of complexity, which will be expressed as a dimensionless quantity.[19] This argumentation is threefold:

First, the number of relevant entities contributes to the complexity of an intelligence problem. This part of the argument is based on the information-geometric class of complexity measures introduced by Ay et.al.[20] and especially their insights on how complexity should scale with system size.[21] Their work mathematically explains the logic that complexity increases monotonically[22] with the number of elements (i.e. entities).[23] They also present two exceptions wherein complexity does not increase in line with the number of entities: 1) when an additional entity is added without interactions with other entities, and 2) when two identical sets of entities and interactions are unified into a single system. Both exceptions are interesting but irrelevant for intelligence problems, where exact copies of entities do not exist and wherein non-connected entities simply fall outside the

delineation of the intelligence problem. So, in the case of intelligence problems, any increase of number of relevant entities, increases the level of complexity.

Second, the complexity of an intelligence problem only scales with the number of entities that are 'relevant'. The complexity of an intelligence problem focussing on a cyber-attack does not scale with the size of the bottle of 'Club Mate' soda the hacker is drinking, even though all individual molecules in the drink can be considered entities that interact with each other and the hacker in question.[24] Similarly the complexity of an intelligence problem focussing on a military conflict does not scale with the size of an individual battalion, even though all soldiers within the battalion can be considered entities that interact with each other and the rest of the conflict. This is because the analyst in this case is only interested in the hacker and the battalion as a whole, the way these two sub-systems are organised exactly is not relevant. Weaver calls such sub-systems 'disorganised complexities' that can be solved using statistics.[25] What Weaver calls 'organised complexities' are what this article considers true complexities, which are systems that consist only of entities in whose individual positions you are interested in at any time and thus can be considered 'relevant'.[26] But how to aggregate each sub-system to a level on which they are relevant is a tricky business, since too much aggregation can lead to over simplification of a complex intelligence problem. Ando et.al. luckily provides us with a robustly argued set of conditions that will help to make an 'approximation of useful aggregation' of the system being analyzed, these conditions are: 1) the entities can be aggregated/classified into a smaller number of sub-systems; 2) the interactions within the sub-systems can be studied as though the interaction among sub-systems did not exist; and 3) the interactions among the sub-systems can be studied without regarding the interactions within each sub-system.[27] Each sub-system fulfilling these conditions can be considered a relevant entity, the level of aggregation of each entity can vary within a single intelligence problem (e.g., individual dictator interacting with a certain government).

Third, when approximating the complexity of an intelligence problem, one should not only focus on the number or relevant entities. The number of interactions among the relevant entities should also be taken into account to practically capture the 'complexity aspect' resulting from 'interacting entities' mentioned in the previous section. Figure 1 conceptually visualizes how complexity scales with the number of relevant entities and the number of interactions.

Finally, it is important to stress, that estimating the number of relevant entities and the number of interactions is just an approximation of the level of complexity and in no means a way to precisely

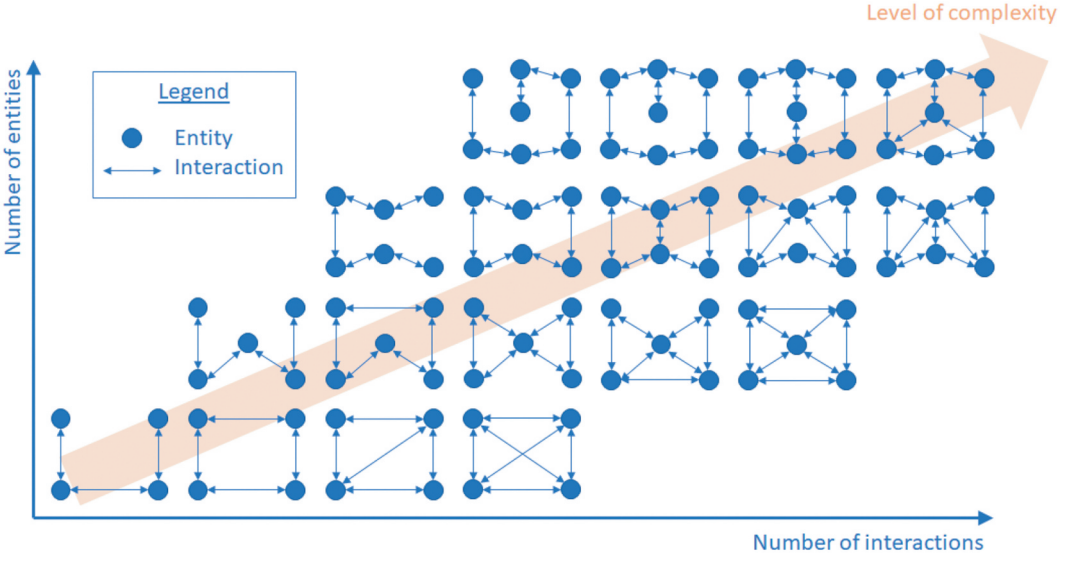

Figure 1. Conceptual visualisation on how complexity scales with number of relevant entities and their interactions.

measure complexity. A more precise measure of complexity, like the ones studied and developed by Ay et.al., requires the identification of the existence and nature of every entity and their interactions that are part of the intelligence problem. Such a detailed picture on the intelligence problem is practically impossible to obtain, for reasons that will be discussed later in more detail.[28] However, it is possible to provide a useful estimate on the orders of magnitude of the number of entities and their interactions. Going forward in this article, the complexity of intelligence problems will be discussed generally in relative terms, i.e. the complexity of one intelligence problem compared to another. So, for this discussion, the ability to precisely determine the level of complexity of an intelligence problem, is not as important as being able to establish that the level of complexity differs based on the number of relevant entities and their interactions.

Complexity determined by the subject of an intelligence problem

The number of relevant entities and their interactions – thus the level of complexity – varies per subject that is being investigated by the intelligence service. For example, the investigation of a single foreign intelligence officer is less complex than the investigation of the foreign policy of a certain state, simply because there are fewer relevant entities and interactions. Whether the intelligence officer is very security-aware and therefore difficult to investigate does not add to the complexity though, since this does not increase the number of interacting entities. Denial and deception do not increase the complexity of an intelligence problem, however it can make an intelligence problem difficult to investigate. Thus, complex ≠ difficult and vice versa simple ≠ easy.

It is important to realize that the subject and its number of relevant entities and interactions can differ significantly depending on the perspective of the intelligence analyst. For example, a threat assessment on how likely a terrorist attack will originate from a certain extremist movement is less complex than attempting to identify which extremists are planning an attack. This is because in the latter case each individual extremist is a relevant entity that is interacting with its surroundings in an organized way, whereas for the general threat assessment the individual extremists can be aggregated to sub-systems or even to the entire movement as a disorganized whole. This is why not every political intelligence problem is more complex than every counter-intelligence problem, although depending on the topic they are working on it is likely that some teams/analysts are more often confronted with high complexity intelligence problems than others.

Complexity determined by the type of assessments

In this sub-paragraph will be discussed how the type of assessment determines the number of relevant entities and interactions (i.e. complexity) in an intelligence problem. As described in the introduction there are multiple different categorizations of intelligence assessments available in literature and it is possible to reflect on these categorizations and explain which of these types of assessments have to take more entities and interactions into account and are thus more complex type of assessments. However, to highlight the interrelation between types of assessments and to allow insights of this study to be translated into practice, a new categorization of intelligence assessments has been formulated. This categorization is mutually exclusive, exhaustive, and formulated from a practitioner's perspective. It distinguishes three types of assessments: *Source assessments, Situation assessments* and *Effect assessments*. These three types of assessments will be explained using the 'secrets, puzzles and mysteries' metaphor widely discussed in literature on intelligence analysis.[29] This metaphor has its limitations when used as a categorization of intelligence assessments or intelligence problems (see also the next section), but nevertheless, its imaginative power remains useful to convey the concepts of intelligence analysis.

Source assessments lead to an estimation by the analyst on how likely the obtained intelligence is true, the obtained intelligence can be something that was meant to be 'secret' but can also be publicly available information (OSINT). In line with NATO guidelines (aka Admiralty Code), such assessments

would include source evaluation and evaluation of the source itself.[30] Preferably also the 'proximity' of the source and the origins of the information – first hand, second hand, etc. – is taken into account.[31]

Situation assessments lead to a description of a past or current situation and a likelihood estimation of its actual occurrence. The obtained pieces of intelligence, including its source assessments, are pieces of the 'puzzle' that together describe the past or current situation the intelligence service is investigating. The challenge is that situation assessments are, as Gentry puts it in the metaphor, puzzles whose 'colour and pattern schemes are hard to discern, the puzzle has many pieces, several of which are missing, and other pieces have been damaged or discoloured, perhaps purposefully'.[32] **Effect assessments** lead to insights on the consequences of the situation assessment. Such insights are basically descriptions of possible future situations with an estimated risk of occurrence. The risk of occurrence consists out of an estimation of the *likelihoods* the current situation is changing in such a way the possible future situations will occur, and the *impact* these situations have on the interests of the end-user (e.g., threat to national security). Such assessments are the 'mysteries' of the above-mentioned metaphor. They are mysteries because the future situations and their effects on national security are the results of a large variety of interactions between multiple individuals with bounded rationality. Therefore, it is theoretically impossible to provide an effect assessment that is confirmed. However, since the future is the result of past events, intelligence services can provide useful assessments on what might happen based on what is known about all relevant past and current situations.[33]

Basically, effect assessments require a set of situation assessments, and situation assessments require a set of source assessments. Thereby exponentially stacking the number of relevant entities and their interactions. This means that for a specific subject the source assessments are less complex than the situation assessments which are less complex than the effect assessments (i.e. complexity of source assessments < situation assessments < effect assessments). Only for a specific subject, because a situation assessment on a very complex subject (e.g. the security situation of a country that is in the midst of a civil war) can be more complex than an effect assessment on a relative simple subject (e.g. future travel movements of a foreign terrorist fighter).

To visualize the stacking of assessments the *IDEF0 modeling method*[34] is applied to provide a simplified description of the intelligence process in Figure 2. Note though that the actual intelligence analysis process is not as linear as it is depicted, but rather it is a continuous process with a variety of iterations around and between assessments.[35]

Influence of the level of complexity on intelligence analysis

Introduction of a ratio scale for complexity of intelligence problems

To indicate the effects of complexity on intelligence analysis, this article will build up step-by-step a diagram in Figure 6 that indicates how the ratio analysis/intelligence changes for more complex intelligence problems. Starting with the level of complexity on a continuous scale with a dimensionless quantity, see Figure 3. Thereby adapting the nominal and ordinal scales mentioned in the previous section, including the 'secrets, puzzles and mysteries' metaphor into a ratio scale that includes the two aforementioned complexity factors (type of analysis and nature of subject). The value of expressing complexity on a ratio scale is that it makes the categorizations less ambiguous and allows for more precise differentiation among intelligence problems. Additionally, the ratio scale can also accommodate the category that Treverton added to the ordinal scale which he called 'complexities', which are basically intelligence problems with a very high level of complexity and thus at the top of the ratio scale.[36]

Exponential increase of relevant intelligence available in the world

For every added relevant entity to an intelligence problem, the number of possible interactions increases exponentially and therefore also the absolute amount of relevant intelligence available in

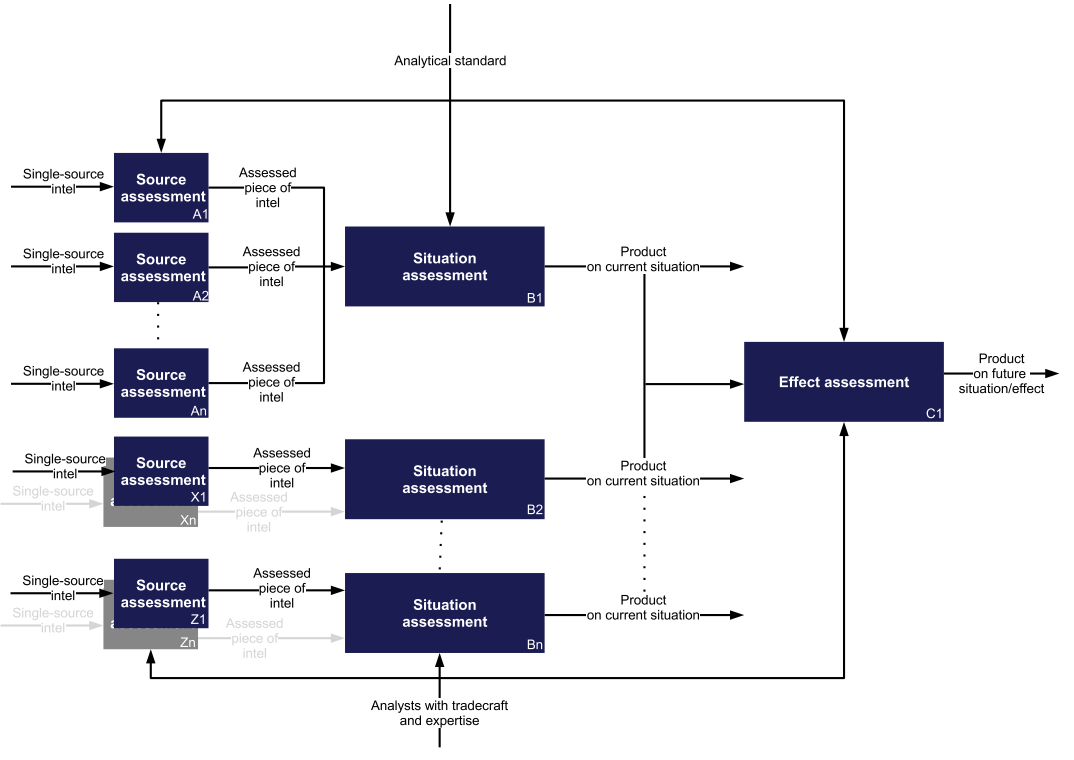

Figure 2. Simplified IDEF0 description of the intelligence analysis process.

Figure 3. Scale of complexity.

the world. In order to have all the relevant intelligence of an intelligence problem, you need to have intelligence on every relevant entity and every possible interaction, including the intelligence indicating there is no interaction between two specific entities. Therefore, the total amount of relevant intelligence available in the world increases exponentially, as a triangular sequence,[37] for every increase of complexity of an intelligence problem.[38] The exponential increase of relevant intelligence available in the world is indicated by the black line in Figure 4.

Exponential increase of the intelligence gap

The increase of complexity of an intelligence problem also exponentially increases the size of the intelligence gap between the *available* relevant intelligence and the *collected* relevant intelligence. This is the result of two factors whose effect on the intelligence gap exponentially increases along the scale of complexity: 1) Collection deficiency and 2) Collected noise.

Collection deficiency

For very simple intelligence problems, with only a few entities and interactions, it is possible to collect a near to total intelligence picture.[39] It is even possible that the amount of collected intelligence exceeds the total amount of available intelligence that is relevant, for reasons described

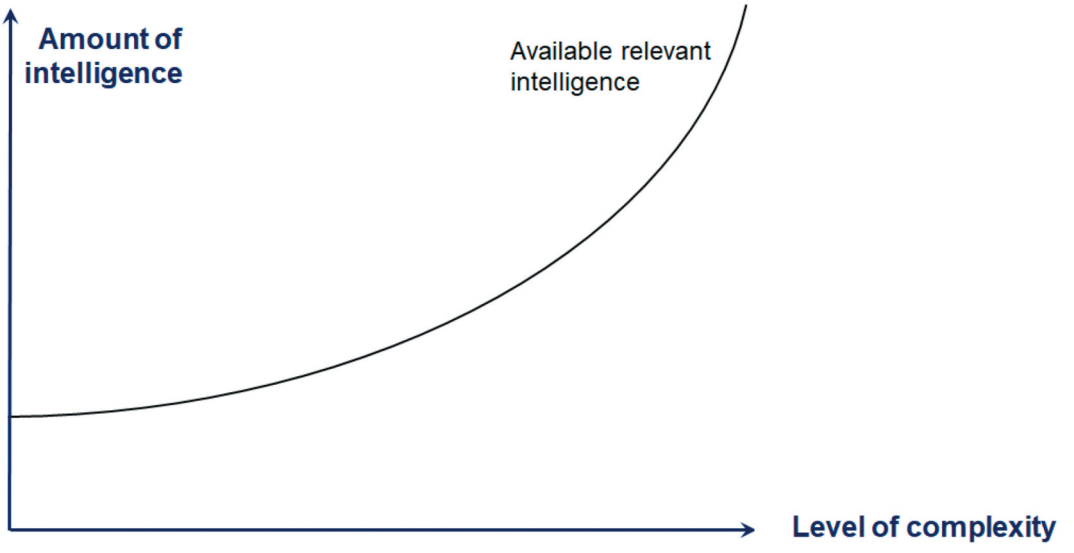

Figure 4. Exponential increase of available relevant intelligence.

in the next paragraph. However, the ability of intelligence and security services to collect a near to total intelligence picture diminishes exponentially when intelligence problems become more complex, mainly due to the practical limitations to collect intelligence on the exponentially increasing number of relevant entities and possible interactions.

Ironically the absolute amount of actually collected intelligence, indicated with the blue line in Figure 5, generally also increases exponentially for more complex problems. Because there are exponentially more entities and possible interactions there is more low hanging fruit to be collected (basic database checks, OSINT, etc.). But because of the practical limits to collection the exponential increase of collection will always be less than the exponential increase of available relevant intelligence, as indicated by the exponentially increasing distance between the blue and black line in Figure 5.

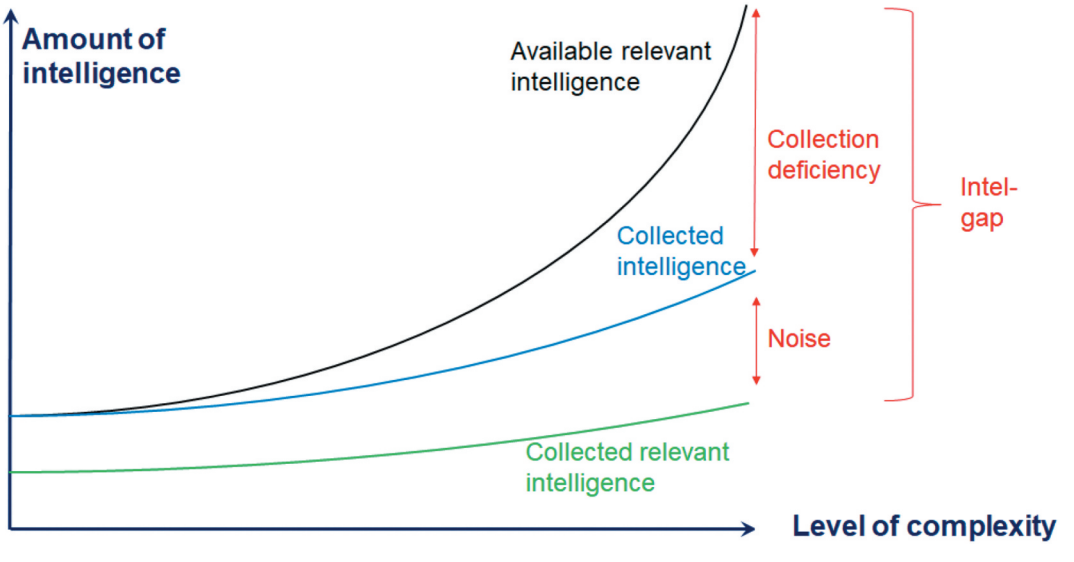

Figure 5. Composition of the intelligence gap.

Besides the practical limitations, it is important to note that there are also theoretical limits to the ability to collect a near to total intelligence picture, which relates to the challenges of perspective observations described by Dent.[40] These are measurement and inquiry challenges surfaced by complexity theory. An important one of these challenges, translated to intelligence and security services, is the interaction between the collection and the subject on which intelligence is collected. To ascertain the influence of that interaction on the entity the service needs to collect intelligence on that subject (if the situation even allows it), causing a new interaction, etc. Basically by collecting intelligence, a service creates new relevant intelligence that is yet to be obtained, an infinite loop that can only be stopped when you decide to assume that the collection itself had no interaction with the subject. Such an assumption contributes to the intelligence gap.

Noise of intelligence collection

If you want to direct the intelligence collection in such a way that only relevant intelligence is collected, you need to have full control and understanding of the intelligence problem that is being studied. Only then, the actions and interactions of every entity can be accurately predicted in order to collect only from the relevant entities at the right times and at the right locations. Since intelligence collection in situations of full control is irrelevant, it is safe to assume that there is always a possibility that irrelevant intelligence is collected even though the collection was directed as much as possible. The likelihood of this increases exponentially when intelligence problems are more complex, because exponentially fewer entities and interactions are fully controlled. It is for example easier to effectively direct intelligence collection on a single known domestic extremist than on an extremist organization abroad with an unknown number of members.

After the collection of intelligence, an analyst can judge the relevance of the intelligence with the current understanding of the intelligence problem as a frame of reference. This means that when little is known about a certain intelligence problem, it is not possible to accurately identify which pieces of collected intelligence are relevant (signal) and which are irrelevant (noise). As intelligence is collected and assessed the understanding of the intelligence problem should improve, leading to more directed intelligence collection and more accurate assessments on relevance, limiting the level of noise iteratively. However, the more complex an intelligence problem is, the less likely/feasible it is that an analyst will ever completely understand every relevant entity and interaction of the intelligence problem. Therefore, more complex intelligence problems are prone to more noise, regardless of how long investigations have been going on. This effect is also exponential, in line with the exponential increase of collecting noise, which is indicated by the exponentially increasing distance between the green and blue line in Figure 5.

Exponential decrease of certainty for more complex intelligence problems

As a result of the exponentially increasing size of the intelligence gap (deficiency and noise), the certainty of analysis decreases exponentially for more complex intelligence problems. Since analysts are basically filling the intelligence gap with assessments, the complete picture of very complex intelligence problems will strongly be based on assessments (see Figure 6). Such assessments can accurately fill the intelligence gap, but the analyst cannot know this for sure without the actual intelligence confirming the assessments. These uncertainties add up for all the assessments made to fill the intelligence gap and increase the degrees of freedom that all assessments have to take into account, exponentially decreasing the level of certainty that can be provided. Thereby concluding the argument that the complexity of an intelligence problem determines to a great extent the certainty that can be provided by intelligence and security services.

'To a great extent' and not completely because there are also other parameters of intelligence problems that influence the level of certainty that can be provided by services. Especially the intelligence position in the intelligence problem. If the collection is positioned effectively on the most influential aspects of the intelligence problem, it is possible to achieve higher levels of certainty even for very complex intelligence problems. However due to the chaotic nature of complex systems,

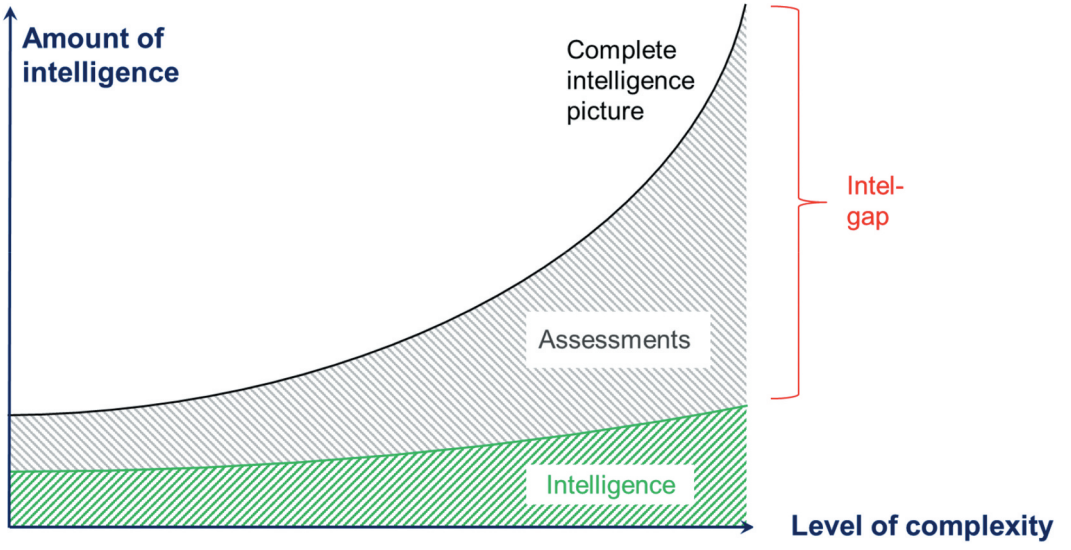

Figure 6. Ratio intelligence and analysis.

seemingly less influential aspects of an intelligence problem can completely change the situation over the course of time.[41] Therefore, the assessments for complex intelligence problems based on effective positioned intelligence sources are only valid for a short period of time. This means that mid- to long-term effect assessments with high certainty on complex intelligence problems will be rare.

Validation of argument

A study of actual intelligence products of the AIVD supports the argument that the complexity of an intelligence problem determines to a great extent the certainty that can be provided by intelligence and security services. This study listed every situation and effect assessment of every regular written intelligence product[42] in a complete month[43] totaling 217 assessments. The assessments with the highest likelihoods were selected according to the analytic standard of the AIVD, which appeared to be only situation assessments.[44] Furthermore, all 217 assessments were categorized on the estimated number of relevant entities, to indicate the level of complexity of the addressed intelligence problem. Taking into account the expected exponential differences in size, the study used the following categories: *Around one relevant entity; Around ten relevant entities; Around relevant hundred entities; Around a thousand or more relevant entities*. This resulted in the graph presented in Figure 7 that shows the ratio of confirmed assessments/total assessments for each category. As the graph indicates, the relative number of confirmations decreases for assessments made on more complex intelligence problems. Apparently AIVD analysts had to fill in larger intelligence gaps with their assessments as intelligence problems became more complex. Assuming all assessments in the intelligence products were correctly executed, this exercise supports the argument that complexity determines to a great extent the certainty that can be provided by intelligence and security services.

Implications

As mentioned in the introduction, the public value services can provide depends on the complexity of the intelligence problem. Intelligence problems that are relatively simple are more suitable for interventions since analysts can provide relatively certain assessments on such problems, one of the

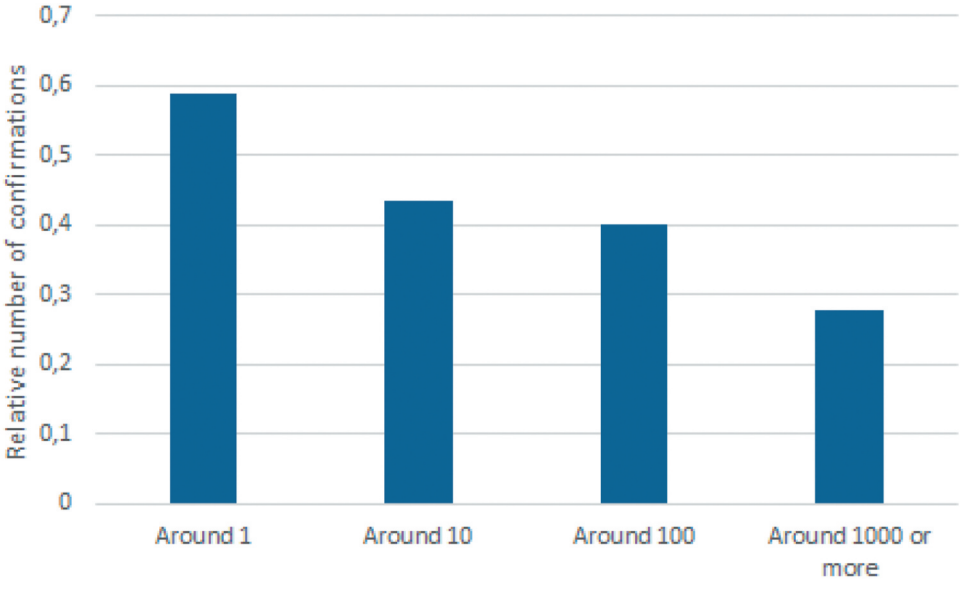

Figure 7. Certainty assessments per size of subject.

essential criteria to make intelligence 'actionable'.[45] Such assessments are certain enough to be assured no action is required, or can be used as a starting point for legal investigations, directions for disruptive (military) operations, an advantage in (diplomatic) negotiations, etc. As the intelligence problem becomes more complex, the assessments become less certain, thus less 'actionable'. Such assessments serve a different purpose, a different public value. It provides 'understanding' of a certain subject, that identify new phenomena, drivers, etc. or explains existing ones. Less actionable, but not less valuable because it has an even wider impact by informing policymakers or even the public. Furthermore, a better understanding of a certain subject also supports the above-mentioned interventions by providing context. It is important to note that the level of complexity is not either very low or very high, the bulk of the intelligence problems (situation and effect assessments) are likely to be somewhere within that bandwidth of complexity. Therefore, it makes sense that the analysis of a single intelligence problem can result both in 'actionable' intelligence and intelligence that provides 'understanding'. This article will discuss in the following three sub-paragraphs, respectively, how intelligence and security services, intelligence clients, and legislators should deal with the varying complexity/public values, to be effective. To explain this, the article consequently uses examples of relatively simple and relatively complex intelligence problems. The examples purposefully cover several topics, to indicate that the implications apply to the entire range of intelligence problems intelligence and security services can be tasked with.

Intelligence collection and analysis

To be effective, intelligence and security services should assess the complexity of an intelligence problem at the start and use it as input for determining the collection strategy and the analytic approach. Intelligence problems that are relatively simple can be approached from the 'positivist' perspective discussed by Walsh.[46] This means that collection can be aimed at obtaining direct or indirect coverage on all relevant entities, driven by opportunity and prioritized on expected gain. Based on this collection, analysts can describe current or previous activities of targeted actors, with a certain likelihood. For example, when trying to ascertain whether a certain regime used chemical weapons in a certain attack, collection should be aimed at all entities involved in the attack

(attackers, victims, contaminated objects, etc.), driven by opportunity and expected gain. The resulting assessment can be a description that the regime possibly used chemical weapons, but it is as likely that it has been made up for propaganda purposes. Collection should then continue until there is sufficient certainty to decide whether repercussions (e.g. sanctions) are appropriate or not. Or until the problem became irrelevant, for example because the regime itself has been toppled. Suitable Structured analytic techniques (SAT)[47] for such assessments are the ones focused on diagnostics, like 'Analysis of Competing Hypotheses'. Supported with a sensible application of contrarian and imaginative SAT's.

Intelligence problems with a relatively high level of complexity should have a different aim and require a different collection strategy and analytic approach. Relatively complex intelligence problems can be more effectively approached from the 'interpretivist' perspective discussed by Walsh.[48] This means that there should be collection that is in-depth and aiming at identifying relevant dynamics, driven by opportunity and expected gain. But at the same time, there should also be collection that is more superficial but more widely spread and driven by obtaining a representative coverage on the entirety of the targeted actors regardless of opportunity to limit collection bias. Based on both types of collection, analysts should be able to identify phenomena, drivers, cause-effect relationships, etc. and be able to assess how significant these influence the targeted actors and their behavior. For example, when trying to understand whether the regime will continue to use chemical weapons, collection can be aimed in-depth on the decision-makers within the regime's military organization and at the same time more superficial at for example the regime's foreign affairs department, propaganda organization and citizens. Based on this collection, analyst can identify: what the military's rationale behind using chemical weapons was (based on in-depth collection) and to what extent future use of weapons is supported or limited by actions of its adversary, by internal-politics and by public opinion (based on a wider spread collection). This can then be used to assess overall, how likely the regime will continue to use chemical weapons, for which the certainty is likely limited (due to the complexity even the regime's leadership itself cannot be certain). More important is to understand, what influences the likelihood of future use of chemical weapons and thus what policies limits or incites the use of such weapons.

Practically, the above-mentioned implications mean that more complex intelligence problems require collection of 'insights' to cover the wider intelligence problem, besides the traditional secretive collection on targets. The collection of insights can be done through analytic exchanges with (foreign) partner services and intelligence clients, but also through analytic exchanges outside the intelligence community with relevant entities themselves and outside experts, preferably through public partnerships in the broadest sense.[49] In the example of the chemical weapons, this would be analytic exchanges with partner services, possibly even directly with the regime's service, but also with experts on the local culture and history of the country. This means for analysts that, more complex intelligence problems, require a direct involvement in the collection of insights but also different analytic approaches. First, a larger dataset of intelligence should be analyzed which requires proper information management and well-designed queries (digital and analog). Second, because 'understanding' is the aim of the analysis, suitable SAT's are focused on modeling of the intelligence subject, like causal-loop diagrams, scenario-techniques, social network analysis and Agent-Based modeling.[50] Finally, analysts should be aware that observations of more complex intelligence problems are even more prone to biases. After all, these biases originate from cognitive heuristics which are 'mental shortcuts adapted over time to enable rapid interpretation of our complex environment'[51] (i.e. the cognitive heuristics are the first responders to filling the intelligence gap).[52] This means that the analyst should address their own biases, the biases of sources (especially the ones providing 'insights'), the biases of everyone involved in the collection and the biases of intelligence clients. To address biases as much as possible, analysts can make use of SAT's to make analyses explicit and allow a sensible application of contrarian and imaginative SAT's.[53] For complex intelligence problems, it is especially useful to apply SAT's together with intelligence clients, as a way

of obtaining their insights but also as a way of conveying the understanding whilst limiting their biases as much as possible too. Furthermore, it is also helpful for analysts to be aware of the value of (cultural) diversity to limit such biases, both from the side of colleagues as from the side of sources (like experts and other services).[54]

Intelligence clients

To effectively direct the services and judge their performances, intelligence clients should take the complexity of intelligence problems into account. Depending on the intelligence problem, intelligence clients can be policymakers and/or executive services (possibly operating within the same service but outside the intelligence cycle), but also the public and end-users inside the intelligence service (case officers, operators, etc.). All these intelligence clients serve different public values and benefit differently from 'actionable' intelligence and intelligence that helps them 'understand'. To task services effectively, it is important that intelligence clients align the complexity of intelligence problems with their expectations of what public value the service should provide, and with the capabilities of intelligence clients to follow up on what the service delivers. For example, policymakers can task services to investigate as many individual financiers of terrorist organizations as possible (many individual intelligence problems) to financially weaken a certain terrorist organization. If the terrorist organization has a clear organizational structure with defined membership and the targeted financiers are operating within national borders, it can be expected from services to provide assessments on financiers with high likelihood on which the public prosecutor and police can organize interventions. If the terrorist organization is more ambiguous without formal membership and/or many non-formal affiliated members the intelligence problems are more complex because this expands the width of entities that can be possible affiliated members and requires more depth collection to identify whether the non-formal members can actually be considered affiliates and whether the targeted financier is wittingly financing the terrorist organization. This is possible to achieve, since it is still not a very complex intelligence problem and can be compensated by a larger investment of capacities. But if the financiers would operate from other countries, or even operate with involvement of these host countries, the intelligence problems are exponentially more complex. Somewhere in that bandwidth of complexity, it becomes reasonably impossible to compensate the increasing complexity with larger investments or capacities, and/or it becomes too complex for the public prosecutor and police to be able to effectively follow up on the provided intelligence assessments. In such situations, it would have been sensible for the policymaker and the involved services, to prioritize the investigation of how the financing of a specific terrorist organization works. A better understanding of these dynamics can possibly lead to a new policy that is more effective in financially weakening the terrorist organization and it can provide the necessary context for public prosecutor and police to operate. It is worth noting however, that the complexity of the policies or interventions also add to the intelligence problem as a whole in the case of ex-ante assessments. So, an ex-ante assessment on the consequences of an arrest of a single terrorist financier can provide more certainty than an ex-ante assessment on the consequences of publicly sharing how the financing of a certain terrorist organization works.

Aligning the complexity of the intelligence problem effectively with the expected public value and the follow-up capabilities of intelligence clients requires some precision though. The value of formal directives and comparing the performances using standardized reporting diminishes if it covers intelligence problems over a wider bandwidth of complexity. Continuing in the same example, a formal directive for services to investigate financiers of all terrorist organizations which are a threat to national security and compare the results of the investigations has limited value. Nor would it be useful to direct services to investigate how the financing of all these terrorist organizations work. Terrorist organizations vary in complexity, which means that the service will deliver different results per organization and the value for intelligence clients will vary based on their capabilities to follow up on what services has provided. Practically this means that there is also no

value in comparing the number of intelligence reports between analysts, teams, and services if there are significant differences in the complexity of the intelligence problems they investigate. It might sound counter-intuitive, but investigations of more complex intelligence problems likely produce higher number of intelligence reports as the absolute number of collected relevant intelligence on which reports can be written should be higher (see the green line in Figure 5).

Intelligence legislation

Legislation should also take into account the varying levels of complexity of intelligence problems. Since the concept of intelligence investigations is often compared to legal investigations – the latter are likely on average significantly less complex – there is a risk that intelligence and security acts are disproportionally limiting the ability of services to address the above-mentioned implications of more complex intelligence problems. For example, limiting exchanges with other services (nationally and internationally) because they operate under a different legal framework makes sense in relatively simple intelligence problems wherein exchanges imply sharing of (technical) selectors on individuals. But exchanges for relatively complex intelligence problems focus also on exchanging insights, which adds more (cultural) diverse insights that limit biases of all involved in the exchange.

Furthermore, in line with the main argumentation of this article, the complexity of intelligence problems determines to a great extent the certainty that can be provided in legal argumentation. The legal argumentation required to collect intelligence on a target and retain collected intelligence, depends strongly on how certain a service is that the specific target has insight and/or influence on the intelligence problem at hand. The amount of certainty a service can provide in such argumentation, and even the relative amount of insight and/or influence a target can have, diminishes exponentially for more complex intelligence problems. For example, the legal argumentation on how the intelligence collection on a certain individual will provide essential insight proportionate to the privacy impact, will likely include assessments of higher certainty if that individual is expected to be involved in conducting cyber-attacks, than if that individual is expected to be aware of the strategy behind cyber-operations of a certain organization. Whether someone is involved in conducting cyber-attacks, can be difficult to establish, but it is not a very complex problem. At least, not compared to understanding how the strategy behind cyber-operations of a certain organization is developed. The development of such a strategy can be the result of many interactions of individuals within and outside the organization, including actions of the actors that are targeted by the cyber-operations, possibly no one within the organization is fully aware on how their strategy if developed and how effective it will be.

Practically, legislators are recommended to investigate to what extent their specific intelligence and security acts allow services and oversight to take the complexity of intelligence problems into account, in order to identify whether legislation is actually disproportionally limiting the ability of services to investigate complex intelligence problems. Especially because this can lead to more unnecessary infringements of privacy and civil liberties in the long run, as proper investigations of complex intelligence problems can provide indicators and contra-indicators that helps to determine whether investigations and interventions on relative simple intelligence problems are proportional. For example, if there is a good understanding of the strategy behind cyber-operations of a certain organization, and it becomes clear that only long-term members are involved in offensive cyber-operations and the rest is just 'hobbying', then the duration of membership can be used for the decision whether intelligence collection should continue or quit. Such insights cannot be gained if intelligence is only collected on individuals that are with a high certainty connected to offensive cyber-operations, also it would reinforce the collection bias toward known individuals.

It is important to note though, that the article is not arguing for legislation that is exclusively congruent with relatively complex intelligence problems. This line of reasoning might allow too much collection for relatively simple intelligence problems and risks eroding the rule of law that democratic embedded intelligence and security services are tasked to uphold and protect.

Legislation and oversight should therefore allow for the possibility to vary on a case by case basis the legal requirements proportionate to the level of complexity of the intelligence problem.

Future research

As argued above, the level of complexity of intelligence problems should be considered from a methodological, client, and legal perspective. To support further research on all three aspects, it would be useful to research how to estimate more precisely the level of complexity of an intelligence problem without decomposing the continuous scale into an ordinal scale that is not able to reflect the exponential effects of increasing levels of complexity.

Additionally, it would be valuable to develop a practical framework that can be used by intelligence analysts to determine which SATs are useful to apply depending on the complexity of the intelligence problem. It would make the most sense to integrate the concept of complexity into existing frameworks that already take other aspects into account. While this article has provided some insights on the use of SATs in intelligence problems of varying complexity, it would require some thorough evaluation to determine which SATs are actually (the most) effective in intelligence problems of a certain complexity. This could also lead to insights on how certain SATs should be applied differently depending on how complex the intelligence problem is that is being analyzed.

Furthermore, the broader body of science on complexity and complex adaptive systems has still a lot to offer to intelligence studies and services. From a theoretical perspective, for example, insights on dynamics inherent to complex systems (e.g. chaos and bounded rationality) can provide frameworks for historical analyses on the actions of intelligence services, including intelligence failures. But also, from a practical perspective, for example analytic tools like agent-based modeling that can support the identification of type of dynamics/threats that might occur in the future but have not occurred in the past. Such dynamics are typical for more complex intelligence problems and key to identify if one wants to limit 'unknown-unknowns' (e.g. unidentified attack plans), a key task of intelligence and security services.[55]

Finally, it is important to stress that the level of complexity is not the only parameter of an intelligence problem that significantly influences intelligence analysis, others include *availability of obtained intelligence* and *vulnerability of obtained intelligence*. Further research is required to identify these additional parameters and determine the interrelations between the parameters and its (individual) influence on intelligence investigations from a methodological, client, and legal perspective.

Notes

1. Kent, *Strategic Intelligence for American World Policy*; and Davis, "Profession of Intelligence Analysis".
2. Zohar, "Intelligence Analysis as Grounded Theory"; Walsh, "Improving Strategic Intelligence Analytical"; and De Valk, *Dutch Intelligence*.
3. Krizan, *Intelligence Essentials for Everyone*; and Vandepeer, *Applied Thinking for Intelligence Analysis*.
4. Vandepeer, *Applied Thinking for Intelligence Analysis*; NATO, *Assessment and Communication of Uncertainty*; Treverton, "Addressing 'Complexities' in Homeland Security"; Pidd, *Tools for Thinking*; Ackoff, "Resurrecting the Future of Operational Research"; and Jones, *The Thinker's Toolkit*.
5. Jervis, *System Effects: Complexity in Political and Social Life*. Even though Complex Adaptive Systems are only mentioned in a footnote, the concepts he applies in relation to complexity draws heavily from this specific subfield of complexity.
6. Weaver, "Science and Complexity"; and Ando, *Essays on the Structure of Social Science Models*.
7. Beebe and Beebe, "Understanding the Non-Linear Event"; and Treverton, "Addressing 'Complexities' in Homeland Security".
8. Hall and Citrenbaum, *Intelligence Collection*.
9. Cederman, *Emergent Actors in World Politics*.
10. Nikolic, Co-Evolutionary Modelling Socio-Technical Systems, 30; Originating from: Maani en Cavana, *Systems Thinking and Modelling*.

11. In line with complex adaptive systems theory, intelligent beings are considered to have internal models that adapt its behavior based on the outcomes of previous interactions. The brain, that contains the internal model of humans, is by itself complex, where the behaviour of a person emerges from the interactions of electrons. The lack of understanding its own brain and the inability to optimize its own internal process, makes the rationality of humans inherently bounded. Opposed to simple command and control systems, like a generic elevator.
12. Chan, "Complex Adaptive Systems"(based on authors John Holland, Stuart Kauffman, Ilya Prigogine and Brian Goodwin); Preiser et al., "Social-Ecological Systems as Complex Adaptive Systems" (based on the articles: Holland, *Hidden Order*; Arthur, "Self-Reinforcing Mechanisms in Economics"; Arthur, Durlauf, and Lane, *The Economy As An Evolving Complex System II*; Levin, "Ecosystems and the Biosphere as Complex Adaptive Systems"; Levin, "Self-Organization and the Emergence of Complexity in Ecological Systems"; Cilliers, *Complexity and Postmodernism*; and Chu, Strand, and Fjelland, "Theories of Complexity").
13. Beebe and Beebe, "Understanding the Non-Linear Event".
14. Ibid.
15. Chan, "Complex Adaptive Systems"; and Preiser et al., "Social-Ecological Systems".
16. Ibid.
17. Chan, "Complex Adaptive Systems".
18. Nikolic, "Co-Evolutionary Modelling Socio-Technical Systems"; Preiser et al., "Social-Ecological Systems"; and Beebe and Beebe, "Understanding the Non-Linear Event".
19. A dimensionless quantity means it is a quantity that cannot be expressed with a standardized unit, opposed to quantities like *time* and *temperature* that can be expressed in the units *seconds* and *degrees Celsius* respectively.
20. Ay et al., "Framework for Complexity Measures"; and Ay et al., "A Geometric Approach to Complexity".
21. Olbrich et al., "How Should Complexity Scale with System Size?" 407–15.
22. Monotonically in this case basically means that there are no situations wherein the complexity decreases while system size increases.
23. They provide mathematical argumentation on how this is the case for the two prevailing complexity measures: the 'excess entropy' of Grassberger and the 'neural complexity' introduced by Tononi, Sporns and Edelman.
24. Club Mate is a caffeinated soda popular in hacker culture, see: Vice.com, 'How a German Soda Became Hackers".
25. Weaver, "Science and Complexity".
26. Ibid.
27. Ando, *Essays on the Structure of Social Science Models*.
28. Also, if you have all this information, the intelligence problem would be rendered useless. Because if you know everything of the subject, then what is the problem?.
29. Borg, "Improving Intelligence Analysis"; Gentry, "The "Professionalization" of Intelligence Analysis"; Hilsman, "Intelligence and Policy-Making in Foreign Affairs"; and Omand, "The Future of Intelligence".
30. NATO, "NATO – STANAG 2511: Intelligence Reports".
31. Krizan, *Intelligence Essentials for Everyone*.
32. Gentry, "The "Professionalization" of Intelligence Analysis," 657.
33. For readers who are familiar with adjacent possible. The intelligence analysts attempts to consider all possible futures (Mt+1) based on the situation assessment (Mt (x)) and based on this makes an effect assessment. In line with Kaufman's formula, complex situation assessments (high value of Mt) will lead to exponentially more complex effect assessments.
34. IDEF0 is a standardized modeling method that can be used to visualize and analyze (business) processes. See: Federal Information Processing Standards Publications, Integration Definition for Functionmodeling (IDEF0).
35. This is a key reason why many, like Hulnick, argue rightly that the traditional 'intelligence cycle' is also not as straightforward as it looks. See: Hulnick, "What's Wrong with the Intelligence Cycle," 961–62.
36. Treverton, "Addressing "Complexities" in Homeland Security," 1–4.
37. For every entity added to the intelligence problem the amount of relevant intelligence increases by one – being the added entity – plus all possible interactions between the added entity and all other entities that are already part of that intelligence problem. This can be expressed as: $\sum^{\frac{n(n+1)}{2}}$ which is known as a 'triangular sequence'.
38. For this article, the amount of intelligence is considered a dimensionless quantity, but if you would consider every raw obtained intelligence report to be a quantity then there is a (large) number of intelligence on every single entity and possible interaction, exacerbating the exponential effect that has been described.
39. Although obtaining a near to total intelligence of very simple intelligence problems is not per se easy, especially when the few entities are actively applying denial and deception tactics.
40. Dent, "Observation Challenges Surfaced by Complexity Theory," 2–9.
41. Nikolic, "Co-Evolutionary Modelling Socio-Technical Systems," 23,25.
42. This is every written product regarding every subject the AIVD actively investigates, subject to tasks A and D of article 8 in the Dutch law on intelligence & security services of 2017. See Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Intelligence and Security Act 2017 [Wet op de inlichtingen- en veiligheidsdiensten 2017].
43. The most recent complete month at the time was chosen, which was November 2019.

44. The analytic standard of the AIVD prescribes the likelihood of information to be judged 'unlikely, doubtful, possibly, likely, very likely or 'confirmed'. Respectively translated from the Dutch: 'onwaarschijnlijk, twijfelachtig}, mogelijk, waarschijnlijk, zeer waarschijnlijk and bevestigd. See Commissie van Toezicht op de Inlichtingen-en Veiligheidsdiensten, 'Toezichtsrapport gegevensverstrekking door AIVD over jihadisten', 27.
45. Martin Havlík, "Actionable Intelligence Supporting Decision-making".
46. Walsh, "Improving Strategic Intelligence Analytical," 552.
47. In the broadest sense and not limited to listings like the 'US Tradecraft Primer of 2009', also not including all these techniques since the value of some are yet to be proven.See US Government, "A Tradecraft Primer'; and Coulthart, "Evaluation of Structured Analytic Techniques".
48. See note 46 above., 552.
49. Walsh, "Improving Strategic Intelligence Analytical"; and Westerman, "Integrating Intelligence Practice and Scholarship".
50. Borg, "Improving Intelligence Analysis"; and De Valk, "Case Studies into the Unknown" (Causal-Loop Diagrams and Scenario Analyses); Koschade, "A Social Network Analysis of Jemaah Islamiyah" (Social network analysis); and Menkveld, "Secret Agents" (agent-based modelling).
51. McCollough, Denmark, and Harker, "Interliminal Design". Based on Tversky and Kahneman, "Judgment Under Uncertainty".
52. McCollough, Denmark, and Harker, "Interliminal Design"; Tversky and Kahneman, "Judgment under Uncertainty"; and Young et al., "Software Complexity".
53. Richards J. Heuer Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, 17–28.
54. Callum, "Cultural Diversity in the Intelligence"; and Jones and Silberzahn, *Constructing Cassandra*.
55. De Valk, "Case Studies into the Unknown", 247–51.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Christiaan Menkveld is a guest researcher and lecturer at the Institute of Security and Global Affairs (ISGA) of Leiden University. His research focuses on the methodology and practical implications of intelligence analysis. He has experience working as a senior intelligence analyst and has a close working-relationship with the Dutch intelligence and security services for the benefit of his academic research.

Bibliography

Ackoff, R. L. "Resurrecting the Future of Operational Research." *The Journal of the Operational Research Society* 30, no. 3 (1979): 189–199. doi:10.2307/3009600.

Ando, A. *Essays on the Structure of Social Science Models*. Cambridge, Mass.: MIT Press, 1963.

Arthur, B. "Self-Reinforcing Mechanisms in Economics." In *The Economy as an Evolving Complex System*, edited by P. W. Anderson, K. Arrow, and D. Pines, 9–31. Redwood City, CA: Addison-Wesley, 1988.

Arthur, W. B., S. N. Durlauf, and D. Lane, eds. *The Economy As An Evolving Complex System II*. 1st ed. Reading, Mass: CRC Press, 1997.

Ay, N., E. Olbrich, N. Bertschinger, and J. Jost. "A Unifying Framework for Complexity Measures of Finite Systems." *Working Paper 06-08-028*, 16. Santa Fe Institute, 2006.

Ay, N., E. Olbrich, N. Bertschinger, and J. Jost. "A Geometric Approach to Complexity." *Chaos: An Interdisciplinary Journal of Nonlinear Science* 21, no. 3 (September, 2011): 037103. doi:10.1063/1.3638446.

Beebe, S. M., and G. S. Beebe. "Understanding the Non-Linear Event: A Framework for Complex Systems Analysis." *International Journal of Intelligence and CounterIntelligence* 25, no. 3 September 1 (2012): 508–528. doi:10.1080/08850607.2012.678687.

Borg, L. C. "Improving Intelligence Analysis: Harnessing Intuition and Reducing Biases by Means of Structured Methodology." *The International Journal of Intelligence, Security, and Public Affairs* 19, no. 1 (2017): 2–22. doi:10.1080/23800992.2017.1289747.

Callum, R. "The Case for Cultural Diversity in the Intelligence Community." *International Journal of Intelligence and CounterIntelligence* (October 29, 2010). doi:10.1080/08850600150501317.

Cederman, L.-E. *Emergent Actors in World Politics*. Princeton, N.J: Princeton University Press, 1997.

Chan, S. "Complex Adaptive Systems." Cambridge, Mass: MIT, 2001. http://web.mit.edu/esd.83/www/notebook/Complex%20Adaptive%20Systems.pdf

Chu, D., R. Strand, and R. Fjelland. "Theories of Complexity." *Complexity* 8, no. 3 (2003): 19–30. doi:10.1002/cplx.10059.

Cilliers, P. *Complexity and Postmodernism: Understanding Complex Systems*. London: Routledge, 1998.
Commissie van Toezicht op de Inlichtingen-en Veiligheidsdiensten. "Toezichtsrapport Nr. 57 over De Gegevensverstrekking Door De AIVD Binnen Nederland over (Vermeende) Jihadisten - Rapport – CTIVD." Rapport, April 24, 2018. https://www.ctivd.nl/documenten/rapporten/2018/04/24/index .
Coulthart, S. J. "An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques." *International Journal of Intelligence and CounterIntelligence* 30, no. 2 April 3 (2017): 368–391. doi:10.1080/08850607.2016.1230706.
Davis, J. "Sherman Kent and the Profession of Intelligence Analysis." Central Intelligence Agency, November, 2002. https://apps.dtic.mil/docs/citations/ADA526587
De Valk, G. "Case Studies into the Unknown - Logic & Tooling." *Romanian Intelligence Studies Review* 21 (2019): 243–268.
De Valk, G. G. D. *Dutch Intelligence–towards a Qualitative Framework for Analysis: With Case Studies on the Shipping Research Bureau and the National Security Service (BVD)*. Netherlands: BJu Legal Publishers, 2005.
Dent, E. B. "The Observation, Inquiry, and Measurement Challenges Surfaced by Complexity Theory." *SSRN Electronic Journal* (2013). doi:10.2139/ssrn.2335850.
Federal Information Processing Standards Publications. Integration Definition for Functionmodeling (IDEF0). Federal Information Processing Standards Publications FIPS 183. Gaithersburg, Maryland, issued, December 21, 1993. http://www.idef.com/wp-content/uploads/2016/02/idef0.pdf
Gentry, J. A. "The "Professionalization" of Intelligence Analysis: A Skeptical Perspective." *International Journal of Intelligence and CounterIntelligence* 29, no. 4 October 1 (2016): 643–676. doi:10.1080/08850607.2016.1177393.
Hall, W. M., and G. Citrenbaum. *Intelligence Collection: How to Plan and Execute Intelligence Collection in Complex Environments*. Santa Barbara, CA: ABC-CLIO, 2012.
Heuer, R. J., Jr., and R. H. Pherson. *Structured Analytic Techniques for Intelligence Analysis*. Washington D.C: CQ Press, 2011.
Hilsman, R. "Intelligence and Policy-Making in Foreign Affairs." *World Politics* 5, no. 1 (October, 1952): 1–45. doi:10.2307/2009086.
Holland, J. H. *Hidden Order: How Adaptation Builds Complexity*. Reading, MA: Addison-Wesley, 1995.
Hulnick, A. S. "What's Wrong with the Intelligence Cycle." *Intelligence and National Security* 21, no. 6 December 1 (2006): 959–979. doi:10.1080/02684520601046291.
Jervis, R. *System Effects: Complexity in Political and Social Life*. Princeton, NJ: Princeton University Press, 1998.
Jones, M., and P. Silberzahn. *Constructing Cassandra: Reframing Intelligence Failure at the CIA, 1947–2001*. 1st ed. Redwood City, CA: Stanford Security Studies, 2014.
Jones, M. D. *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*. Rev and Updated ed. New York: Currency, 1998.
Kent, S. *Strategic Intelligence for American World Policy*. Princeton: Princeton University Press, 2015.
Koschade, S. "A Social Network Analysis of Jemaah Islamiyah: The Applications to Counterterrorism and Intelligence." *Studies in Conflict & Terrorism* 29, no. 6 September 1 (2006): 559–575. doi:10.1080/10576100600798418.
Krizan, L. *Intelligence Essentials for Everyone*. Washington, DC: Joint Military Intelligence College, 1999.
Levin, S. A. "Ecosystems and the Biosphere as Complex Adaptive Systems." *Ecosystems* 1, no. 5 September 1 (1998): 431–436. doi:10.1007/s100219900037.
Levin, S. A. "Self-Organization and the Emergence of Complexity in Ecological Systems." *BioScience* 55, no. 12 (December 1, 2005): 1075–1079. https://doi.org/10.1641/0006-3568(2005)055[1075:SATEOC]2.0.CO;2 .
Maani, K., and R. Y. Cavana. *Systems Thinking and Modelling : Understanding Change and Complexity*. Auckland: [Great Britain]: Prentice Hall, 2000. https://trove.nla.gov.au/version/44094406 .
Martin, H. "'Actionable Intelligence – Supporting Instrument for Commander's Decision-making Process.' [Rychle a Prakticky Použitelná Zpravodajská Informace – Podpůrný Prostředek Pro Rozhodovací Proces Velitelů]'." *Vojenské Rozhledy* 25, no. 1 (2016): 61–72. doi:10.3849/1210-3292.25.2016.01.061-072.
McCollough, A., D. Denmark, and D. Harker. "Interliminal Design: Understanding Cognitive Heuristics to Mitigate Design Distortion." *FormAkademisk - Forskningstidsskrift for Design Og Designdidaktikk* 7, no. 4 (December 16, 2014). doi:10.7577/formakademisk.799.
Menkveld, S. H. C. "Secret Agents: An Exploratory Study to the Added Value of Agent-Based Modeling to the Strategic Geopolitical Intelligence Process of NATO State Intelligence Services." *TU Delft Repository*, 2013. https://repository.tudelft.nl/islandora/object/uuid%3A33d24e8e-059a-4a30-93ef-f256b7e0fa3a
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Intelligence and Security Act 2017 [Wet op de inlichtingen- en veiligheidsdiensten 2017], wetten.overheid.nl§, 2017. https://wetten.overheid.nl/BWBR0039896/2020-01-01
NATO. "NATO - STANAG 2511: Intelligence Reports." Brussels, January 27, 2003.
NATO. *Assessment and Communication of Uncertainty in Intelligence to Support Decision-Making*. STO TECHNICAL REPOR, TR-SAS-114. Brussels: NATO, 2020.
Nikolic, I. "Co-Evolutionary Method For Modelling Large Scale Socio-Technical Systems Evolution." *TU Delft Repository*, 2009. https://repository.tudelft.nl/islandora/object/uuid%3Ab6855afa-e8ab-442d-ac5a-f645f7639c73
Olbrich, E., N. Bertschinger, N. Ay, and J. Jost. "How Should Complexity Scale with System Size?" *The European Physical Journal. B* 63, no. 3 (June, 2008): 407–415. doi:10.1140/epjb/e2008-00134-9.
Omand, S. D. "The Future of Intelligence : What are the Threats, the Challenges and the Opportunities?" The Future of Intelligence, 11 April 2014. https://doi.org/10.4324/9780203071472-2

Pidd, M. *Tools for Thinking: Modelling in Management Science*. 3rd ed. Chichester, U.K: Wiley, 2009.
Preiser, R., R. Biggs, A. De Vos, and C. Folke. "Social-Ecological Systems as Complex Adaptive Systems: Organizing Principles for Advancing Research Methods and Approaches." *Ecology and Society* 23, no. 4 (December 19, 2018). doi:10.5751/ES-10558-230446.
Treverton, G. F. 'Addressing "Complexities" in Homeland Security'. *The Oxford Handbook of National Security Intelligence*, 12 March 2010. doi:10.1093/oxfordhb/9780195375886.003.0021.
Tversky, A., and D. Kahneman. "Judgment under Uncertainty: Heuristics and Biases." *Science* (1974): 1124–1131.
US Government. "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis." *American Psychological Association* (2009). doi:10.1037/e587102011-001.
Vandepeer, C. *Applied Thinking for Intelligence Analysis*. Canberra: The Air Power Development Centre Australia, 2014.
Vice.com. "How a German Soda Became Hackers." Fuel of Choice, February 20, 2014. https://www.vice.com/en/article/xywxm7/how-a-german-soda-became-hackers-fuel-of-choice
Walsh, P. F. "Improving Strategic Intelligence Analytical Practice through Qualitative Social Research." *Intelligence and National Security* 32, no. 5 July 29 (2017): 548–562. doi:10.1080/02684527.2017.1310948.
Weaver, W. "Science and Complexity." *American Scientist* 36, no. 4 (October, 1948): 536–544.
Westerman, I. "Integrating Intelligence Practice and Scholarship: The Case of General Intelligence and Security Service of the Netherlands(AIVD)." *Romanian Intelligence Studies Review* 21 (2019): 243–268.
Young, B. J., G. Booch, J. Conallen, M. W. Engel, K. A. Houston, and R. A. Maksimchuk. In *Object-Oriented Analysis and Design with Applications*. 3rd ed. Addison-Wesley Object Technology Series. Boston, MA: Addison-Wesley, 2007. https://www.informit.com/articles/article.aspx?p=726130&seqNum=4
Zohar, E. "Intelligence Analysis as a Manifestation of a Grounded Theory." *International Journal of Intelligence and CounterIntelligence* 26, no. 1 March 1 (2013): 130–160. doi:10.1080/08850607.2012.705659.