DEALING WITH FUTURE RISKS IN THE NETHERLANDS

Maaïke van Tuyl

The national security strategy is the Dutch government's instrument for multihazard risk management and is intended to contribute to the prevention of societal disruption as a consequence of a (future) disaster or crisis in the Netherlands. It considers the likelihood that a certain incident will occur, the impact if it should occur, and what can be done to prevent the occurrence and/or reduce the impact. In other words, "which threats is the Netherlands faced with, how serious are they, and what can be done to mitigate the consequences?" By annually assessing the likelihood and impact of different scenarios, the government is able to continually improve its overview of risks and to determine priorities regarding the allocation of resources for the prevention of, preparation for, and response to threats. At the start of the annual cycle of the implementation of the national security strategy, possible scenarios are identified. These scenarios are then drawn up and assessed by the Network of Analysts for National Security, resulting in the national risk assessment (NRA). On the basis of this risk assessment, a capabilities analysis is performed. This capabilities analysis assesses whether the country (government, private sector, and civilians) has sufficient capabilities (people, material, knowledge, skills, and procedures) at its disposal to adequately deal with the threat, and it considers which capabilities should be strengthened or developed. Finally, a report is prepared for the council of ministers. On the basis of this report, the cabinet decides which capabilities will be strengthened.*

SAFETY AND SECURITY are the cornerstones of a society in which people feel free, at ease, and connected. In the Netherlands, a densely populated country, disasters can all too easily create a cascade effect. Safety and security can never be guaranteed. A great deal of suffering and damage can nevertheless be prevented through a thorough analysis of possible threats, well-defined prior agreements, and a clear division of tasks.

Strengthening national security is a task for the national government. But a safe and secure living environment in the Netherlands requires everybody's involvement: from

government to the private sector, from international partners to civil society and individual citizens. The Dutch government has tried to optimize preparation for various threats by drawing up a national security strategy.¹ It places the roles and responsibilities of all parties involved in a coherent framework. Central to this strategy is an integrated, whole-of-government approach to national security.

DEALING WITH AN ALTERED THREAT PROFILE

Threats to our security are changing and becoming ever more intertwined. SARS, bird flu, floods, terrorism—these are examples of threats that have demanded more and more

---

*The report and the letter to parliament are publicly available and published on the government website: www.rijksoverheid.nl.

attention in the past few years and that have made us realize our (increasing) vulnerability. Relatively minor threats can, through interdependencies, lead to societal disruption. Think of a flaw in the design of an operating system leading to a disruption of our energy supply. Moreover, the impact of disruptions is increasing. This is caused, among other reasons, by an ever-increasing dependence of Dutch society on critical infrastructures, such as electricity and ICT technologies. Answers to existing and new threats can therefore no longer be formulated and implemented through a single ministry, organization, or (in some cases) even a single country. An integrated and coherent approach that also looks beyond current threats is needed. Planning and policy should not only be based on individual (known) threats, but also on the extent to which overall national security is or can be threatened. Naturally, governments and private parties already play an active role in strengthening security, but in order to be able to effectively direct these efforts, cooperation is needed among all organizations that are responsible for national security: national government, local authorities, civil society, and the business community.

In 2007 the Dutch government developed a national security strategy.[†] The aim of the strategy is to protect society and citizens in Dutch territory against internal and external threats. The strategy is also mindful of the fact that Dutch national security cannot be viewed in isolation from the security of other countries and alliances. Our options for counteracting these threats without cooperating with other countries are limited; an exclusively national approach is insufficient. The rise in sea levels is an obvious example of this, as well as pandemic flu, or the recent tsunami in Japan (2011), which had a major impact on the supply of goods to other countries. International cooperation, both at a bilateral and a multilateral level, is essential for reinforcing national security.

WHAT IS NATIONAL SECURITY?

Dutch national security is at stake when one or more vital interests of our state and/or our society are threatened to such an extent that it might lead to societal disruption. National security encompasses both a threat to security by intentional human actions (security) and a threat caused by disasters, system or process faults, human failure, or natural anomalies such as extreme weather (safety). The goal of the national security strategy is to protect the vital interests of the Netherlands and prevent societal disruption. The 5 vital interests are:

1. *Territorial security*—The undisrupted functioning of the Netherlands as an independent state and, more spe-

cifically, the territorial integrity of our country. The territorial integrity is at risk in the event of, for example, a threat of occupation by another state.

2. *Economic security*—The undisrupted functioning of the Netherlands as an effective and efficient economy. Economic security can, for example, be breached if trade or cultural ties with an important foreign partner are lost.

3. *Ecological security*—Sufficient bounce-back ability of the living environment (flora and fauna) in the event of damage to nature and the environment. Ecological security can be at risk due to disruptions in the management of the surface water, but also due to climate change.

4. *Physical safety*—The undisrupted functioning of humans in the Netherlands and their (living) environment. Physical security can be at risk if public health is threatened by an epidemic, but also if there is, for example, severe flooding or an accident in a chemical factory.

5. *Social and political stability*—The existence of a social climate in which groups of people live together without major conflict within the framework of the democratic state and with shared core values. Social and political stability can be at risk if changes occur in the demographic structure of society (eg, a sudden decrease in solidarity between generations), social cohesion, and the degree of participation of the population in social processes.

The 5 interests are intertwined; a breach of one can lead to the breach of another. For example, breach of physical security can put pressure on social and political stability. At the same time, social and political stability can also be directly at risk.

AN EXAMPLE

The national security strategy assesses threats from various origins. They can be manmade (security), but they can also be caused by organizational failure or natural hazards (safety). Although no biological attacks have occurred on Dutch territory, the Dutch government is aware of biological hazards. The Netherlands consider the probability of a bioattack to be “low” since such an attack requires knowledge of and access to biological agents. The threat of an attack or a real attack, however, would have a serious impact on our national security.² Experiments, incidents, and attacks with biological weapons in the past³ have shown that vital interests such as physical security, social and political stability, and even territorial security can be at stake.

The vital interest of physical security is at stake since it can cause casualties. In Russia, for example, 68 people died after the escape of anthrax from a military laboratory in 1979. Followers of Bhagwan Shree Rajneesh polluted salad bars in Oregon (USA) with *Salmonella* to influence local government elections; 751 people got sick, but no one died. Five people died in the United States after having received anthrax letters in 2001. Several cases of fake anthrax letters

---

[†]The term “national security” encompasses both security and safety.

in the Netherlands have shown that even without a real attack, the threat of an attack is enough to cause considerable social unrest (social and political stability). The impact of an anthrax bomb thrown on the Scottish island of Gruinard, an English military experiment in 1942, shows that even territorial security can be at stake. The island was inaccessible until 1988.

The 5 interests are intertwined; a breach of one can lead to the breach of another. In the examples mentioned, the breach of physical safety (death or injury to people) can put pressure on social and political stability (unrest). Until now, no biosecurity threat has been assessed in the national security strategy. An analysis of pandemic flu (biological but not manmade), however, had the highest score on probability and impact in the Dutch national risk diagram.

THE DUTCH NATIONAL SECURITY STRATEGY

The national security strategy describes the working method for realizing a coherent and integrated approach to national security. The working method aims to deal with ever-changing and developing threats and enables the Dutch government to determine what threatens our national security and how to anticipate those threats. In addition, the Dutch government assumes this method not only enables better substantiated choices in determining priorities and allocating resources, but also allows us to view these choices in their relationship to each other.

The working method consists of 3 phases (see Figure 1):

1. *National analysis of threats and assessment of risks (What could go wrong?)*

In this first phase, a distinction is made between risk analysis and risk assessment. During the analysis, known and new or upcoming threats are identified and scenarios

are developed. This is a medium- to long-term analysis (up to 5 years). These medium-term analyses are then further developed in a thematic in-depth study. For the thematic in-depth study, it is possible to opt for a scenario that can occur in the next 5 years or for a scenario that can occur within a 5-year period situated in the more distant future (eg, in 20-25 years).

The thematic in-depth study results in a scenario that forms the foundation of the national risk assessment (NRA), the assessment of threats in terms of impact to vital interests and likelihood, and the positioning and evaluation of these risks in relation to each other. According to experts on risk governance, the new thing about this approach is the way of thinking about an unsure future. Scenarios are not based on a stockpile of risks that have presented themselves in the past, with enough available data to make a statistical analysis. "The NRA is a 'future based' analysis of possible threats to the national security. And that is a big step forward."⁴

2. *Capabilities analysis (What do we need to have?)*

Based on the risk assessment of all the scenarios that were analyzed, an investigation is conducted to find out:

- What government should be able to do in order to prevent an incident from happening or to reduce the impact of an incident: the tasks; and
- What is necessary to adequately fulfill these tasks: the capabilities?

This strategic planning process determines which capabilities are already sufficiently developed and in place and what can or should be expected from external parties, such as the business community, civil society, and international organizations and, ultimately, which capabilities are not yet developed or need strengthening. These tasks and

Figure 1. The Work Process. Color graphics available online at www.liebertonline.com/bsp

capabilities are then translated into policy options for prevention, preparation, response, and recovery. Finally, a recommendation is drawn up for the council of ministers about which capabilities need to be reinforced.

3. *Policy initiatives (How and where is Dutch national security to be reinforced?)*

The council of ministers decides whether Dutch national security should be improved by reinforcement of capabilities and, if so, by what measures. These political decisions are converted into policy, legislation, and/or concrete actions, depending on the specific capabilities that need to be developed (a few examples are given at the end of this article). Policy implementation of the choices made by the cabinet is not carried out only by the national government. Other public authorities, the business community, and civil society also play an essential role.

ANALYSIS OF THREATS AND ASSESSMENT OF RISKS

In the national risk assessment, threats are measured against a yardstick that applies to all of them. The risk assessment is suitable for an all-hazards approach. In this way, the risks to national security are rendered comparable.

The concept of “risk” is defined as a combination of the “impact” (the total of the consequences of the incident as described in the scenario) and “likelihood” (an estimation about the occurrence of the incident as described in the scenario). Actions or mitigating measures that have already been taken or the societies’ existing resilience are discounted in the assessment of impact and likelihood. We deliberately avoided the traditional “risk equals likelihood times consequence.” First, this way of establishing risks suggests a strictly quantitative interpretation where not all (future) threats are suitable to be assessed in a strictly quantitative manner (eg, the likelihood of radicalization is a qualitative estimation, based on intelligence information). Second, reducing “risk” to a single number conceals 2 fundamental dimensions that should be taken into account when deciding on prioritization and allocation of resources—namely, the impact and likelihood.

Scenario Building

Scenario development offers the opportunity to gain a sense of future uncertainties and factors that should be considered in current decision making. Therefore, the first part of the national security method is the elaboration of scenarios describing incidents that could be a threat to national security in the medium term (up to 5 years). The choice of threats for which scenarios should be written is made partly on the basis of the outcomes of the strategic foresight (potential or upcoming threats with a timescale longer than 5 years). There can also be other reasons—for example,

current developments—for deciding to write a scenario for a certain threat.

A scenario may be used in various ways. This article describes how scenarios are used in the context of the national security strategy and its working method. A scenario offers a way of obtaining a joint picture of future uncertainties and factors that influence decisions that should be made today. In the context of the NRA, a scenario is a description of an incident, the lead-up to that incident and a trigger event (consisting of the underlying cause and any underlying insidious process, and the trigger that actually creates the incidents or brings the insidious process to the surface), the context of the events (indicating general circumstances and the degree of vulnerability and resilience of people, objects, and society), and the consequences of the incident (indicating nature and scale with an overall description of the response and the control measures and consequences of the incident for the continuity of critical infrastructure).

An important initial requisite is that all scenarios are plausible (“it could happen”), but they do not necessarily have to score heavily on likelihood (because the analysis is future-based, scenarios should be “thinkable” but need not have happened already). A second initial requisite for the development of scenarios is that, from the outset, there is an expectation that the scenario will have an impact on a national scale and on at least one of the vital interests (ie, territorial safety, physical security, economic security, ecological security, and social and political stability), to ensure that the scenario deals with a risk to the national security. In addition, the incident scenario must be so specific that it is possible to deduce from it which capabilities will have to be brought to bear in that scenario, and it must take account of existing policy on measures for the various stages in the safety chain. However, that does not mean that all policy is perfect or is implemented flawlessly; it must take account of shortcomings observed or anticipated.

Each of the scenarios in the entire set must be unique and cover the potential scenario scope in terms of risk gradation; the scenarios are “compression points” in the continuum of variations and possibilities. This can be achieved, among other things, per subtheme, by thinking up a number of distinctive variants or totally different scenarios. Scenarios may differ, for example, in scale and intensity of the events, geographical location, likelihood, and possibly other circumstances.

Risk governance experts see advantages in working with scenarios for future-based analysis. But the presentation in a limited number of scenarios has its down sides. The presentation can be easily misinterpreted as an analysis of “sufficiently known and indisputable” security issues,⁵ whereas the NRA is really about interpreting uncertain events. According to risk governance experts, this is not stated clearly enough: “knowledge gaps and conflicts of values are hidden,”⁵ and “The NRA does not advertise that it is an attempt to [...] analyze relevant uncertainties and

discuss them thoroughly. The uncertainty is not visible in the final reports and presentations. Which is—to us—missing out on an opportunity.”⁴

Who Develops a Scenario?

In order to develop a scenario, input is required from various specialist fields. Which specialist fields are involved is determined by the nature of the scenario and its possible consequences. The Dutch government previously covered scenario building and risk assessment, with technical and substantive input from experts. We found, however, that to be able to tap into the most up-to-date knowledge and to diminish (political or policy) bias, a network of analysts should be developed in which knowledge institutions, intelligence services, planning agencies, and scientists from universities and think tanks provide their knowledge and expertise. This Network of Analysts for National Security is now responsible for developing scenarios and conducting our NRA.

Impact Assessment

The impact assessment breaks down into a tangible or quantifiable component (eg, property damage, number of victims) and an intangible more qualitative component (eg, public indignation that may be caused by an incident). The factor of risk perception is also expressly considered in the risk assessment.

The chosen impact criteria for the NRA are an immediate reflection of the objective of the national security strategy: protection of the vital interests of the Netherlands. Each of the 5 vital interests is further specified through impact criteria. The 10 chosen criteria together are considered representative for being able to assess and rank every

possible incident scenario based on impact (damage, loss, cost, etc.). The 10 impact criteria are shown in Figure 2.

The following steps lead to an impact score for a scenario:

- The events and the impact in the scenario are analyzed against each of the 10 impact criteria;
- This analysis leads to the determination of an impact score (label) per impact criterion;
- The 10 individual impact scores are merged using an aggregation procedure into an overall impact score.

The impacts on the different criteria are measured in the same way for all potential incident scenarios. An example: for the estimation of the negative impact on the territory of the Netherlands, it does not matter whether the Netherlands loses authority over Limburg for 2 months due to an occupation by a foreign power, or because the river Maas bursts its banks and all of Limburg is flooded for 2 months. Both incidents are assessed in the same way for this criterion. The difference in assessment of both incidents is expressed in the difference in the assessment of the other impact criteria (eg, violation of the democratic system, damage to the environment, and/or social and psychological impact).

For each of the 10 criteria, the impact is rendered measurable by using 5 categories: A through E, from “limited consequences” to “catastrophic consequences.” Each category is characterized by a range (eg, 0 to 10 fatalities classifies as A).

Likelihood Assessment

Besides determining the impact, the likelihood of the scenario has to be assessed. In some cases, empirical data are available or can be calculated. It is then possible to calculate

Figure 2. The Impact Criteria

the likelihood as a percentage of the incident occurring within the coming 5 years. This way of establishing likelihood is possible for most natural threats (like flooding). In other instances, we can rely only on intelligence data to estimate the likelihood—for example, in cases such as radicalization scenarios. In determining the likelihood of the incident scenario, some initial assumptions are used, including the following:

- To determine likelihood, a breakdown into 5 categories is used (categories A to E). The classification matches the principles chosen to determine impact. Category A represents an incident scenario that is deemed very unlikely, while Category E represents an incident scenario that is deemed very likely. Wherever it is possible to make quantitative estimations, the interval between the categories is (approximately) a factor of 10 for both likelihood and impact. The likelihood is also rendered measurable by using 5 categories A to E.
- The likelihood of the incident scenario is determined by the trigger but also by the consequences (impact) of the incident scenario.
- In determining the likelihood of future risks, incomplete data/information will have to be used to a greater or lesser extent. This means that, depending on the type of incident, more than 1 available information source will have to be used to establish likelihood. Information sources can be: historic (similar) events, statistics (combined if necessary with probability model calculations), failure data (combined with network analyses/decision trees), strategies and actor analyses, and, of course, expert opinions.

Risk Diagram

In order to gain a sense of perspective (Is this risk bigger or smaller than risks we have analyzed before?) and substantiate the priorities set at a later stage, all risks analyzed thus far are presented together in a risk diagram. For each of the scenarios, the NRA returns a score for the aggregated impact and the likelihood. The scores are shown graphically in a risk diagram; an example from our 2011 risk assessment is shown in Figure 3.

The risk diagram can be used to prioritize capabilities that have to be strengthened. The most important viewpoints concerning the information from the risk diagram are:

1. *Risk as a pure function of impact and likelihood*—Based on the classic risk concept, risk is the product of impact and likelihood (in which both are considered equally important). It goes without saying that, in this case, priority is given to the scenarios characterized by a high categorization for impact and for likelihood.

2. *The level of risk of administrative breakdown*—The selection of the NRA scenarios is not random: Only scenarios that pose a threat to national security are important

for the NRA. A subset is formed by the risks with a high chance of administrative breakdown—for example, a major flood or nuclear disaster. This type of scenario is characterized by a (very) low likelihood and a high impact. From the viewpoint of risk of administrative breakdown, the risk is mainly posed by the impact and less by likelihood.

3. *The possibility of risk reduction*—The question of which threat, based on the risk assessment and capabilities analysis, should be given priority not only depends on the risk assessment, but also on the question of which scenarios offer benefits that can be obtained relatively simply: deployment of additional capabilities that would actually diminish the risk. In many cases, this concerns risks with a high likelihood.

However, the downside of the presentation in the risk diagram is that it seems “exact.” Likelihood and impact are not indisputable but the average of expert opinions. The variations in these opinions paint an interesting picture of the uncertainties regarding the risks that were analyzed.⁴ Plotting the range of expert opinions in the risk diagram makes it harder to read for nonexperts, however. Therefore, a separate diagram (with the “bandwidth” of expert opinions) is presented in a supplement to the risk analysis report. Closing the gap between an “easy view” presentation (where all risks are conveniently arranged as “equally known”) and a presentation that clarifies the uncertainties and stimulates discussion on a political level is a challenge for all involved in risk analysis.

CAPABILITIES ANALYSIS

The whole national security strategy is aimed at improving Dutch national security and strengthening society’s resilience. In order to effectively curb a risk, it is possible that extra capabilities need to be developed. A capability may be a skill or knowledge as well as things like measuring apparatus, training, or legislation to prevent dangerous situations. Based on the risk assessment of all the scenarios that are developed and assessed, an investigation is conducted to examine the possibilities of deploying additional capabilities to reduce the impact of a scenario and/or reduce its likelihood. That is done in the capabilities analysis.

The goal of our capabilities analysis is ultimately to increase our resilience to any kind of threat—be it a known and assessed threat or a “black swan.” The capabilities analysis preferably identifies capabilities that have a mitigating effect on more than one type of threat. These so-called generic capabilities are also more likely to be cost-efficient than specific capabilities. And generic capabilities are deemed more likely to help reduce the likelihood and impact of unassessed or unknown threats (black swans) and to make Dutch society resilient to any kind of threat. For instance, evacuation helps diminish the impact of flooding and chemical or nuclear accidents, but also of a new geographically bound disease. However, if the impact or

Figure 3. Risk Diagram. Color graphics available online at www.liebertonline.com/bsp

likelihood of a specific threat is very high, it may also be necessary to develop specific capabilities that reduce the impact and likelihood of this one threat.

Traditionally, the focus in crisis management has been on preparation and response in the government. With the described work process and capabilities analysis, we aim at broadening this scope. Resilience is much broader than the ability to respond to a threat. It is also the ability to prevent a threat from happening altogether, to limit the impact by preventing crippling effects (eg, the disruption of critical infrastructure processes), and to recover from a crisis in order to avoid a lasting societal disruption.

All ministries are involved in this process, as are some interest groups (eg, VNO-NCW, a Dutch confederation of industry and employers). The ministry that is primarily responsible for dealing with the assessed threat leads the capabilities analysis. In order to safeguard a correct use of the methodology and working process, a secretariat is provided by the organization that guards the working method and the national security strategy: the National Coordinator for Security and Counterterrorism.

As noted at the beginning of this article, the government is not solely responsible for our safety and security. Some of the most effective capabilities are not owned or influenced by the government. For example, critical infrastructure such as food, drinking water, and telecommunications are owned by private companies. Because capabilities may be privately owned or can be best developed at local or regional levels, other parties are involved throughout the process of risk assessment and capabilities analysis: private sector and critical infrastructure companies, other bodies of government (eg, local and regional authorities, international organizations such as EU, NATO, and the UN), civil society, and individual citizens. Also, because some capabilities may be relatively new or unknown (eg, social media), up-to-date knowledge from experts on the latest developments is essential.

POLICY INITIATIVES

Not all capabilities mentioned in the capabilities analysis can be strengthened or developed. Budgets are limited, and the positive effects of some capabilities are larger than others. Since 2007 the Dutch government has reviewed annually its priorities related to strengthening its resilience based on the capabilities analyses and the NRA. A few examples:

- The NRA of the occurrence of a pandemic flu (2007-08) showed that such a flu could have crippling effects on the continuous functioning of critical infrastructure processes because of the large number of people staying at home due to sickness, recovery, or caring for family members. As a response, 80% of government organizations and critical infrastructure companies

developed business continuity plans for pandemic situations.⁶

- The assessment of several cyber security scenarios showed that our increasing dependence on ICT technologies also makes us vulnerable to social disruption.⁶ A National Cyber Security Strategy was developed to strengthen Dutch resilience against cyber threats. As part of this strategy, a National Cyber Security Center has been established, where government and the private sector work closely together on a day-to-day basis monitoring, researching, analyzing, and tackling cyber threats and developing security tools.
- The recent analysis of a scenario on satellite disruption caused by a solar storm shows that relatively unknown threats also deserve attention. The disruption of satellite services, used for communication, positioning, and computation of time, can lead to social disruption. Because we know little about the possible consequences of solar storms, the Dutch government in 2012 recognized the need to enhance knowledge and expertise on the impact of solar storms, to develop an early warning system, and to look for ways to create better redundancy.⁷

The Dutch government continues to strengthen the resilience of its society against societal disruption. A key factor in safeguarding our national security is to be able to deal with uncertainties. Risk assessment aims to reduce these uncertainties. Followed by a strengthening of generic and specific capabilities, Dutch resilience to many kinds of threats, both known and unknown, is enhanced.

ACKNOWLEDGMENTS

The author would like to acknowledge the EU project AniBioThreat (Grant Agreement: Home/2009/ISEC/AG/191) for inviting this article for their Supplement. AniBioThreat is a project in the Prevention of and Fight against Crime Programme of the European Union, European Commission—Directorate General Home Affairs. This publication reflects the views only of the author, and the European Commission cannot be held responsible for any use that may be made of the information contained therein.

REFERENCES

1. Minister of the Interior and Kingdom Relations, National Security (letter to Parliament), May 8, 2007, TK 2006-2007, 30821 nr. 3.
2. Magazine Nationale Veiligheid en Crisisbeheersing (Dutch Magazine for National Security and Crisismanagement), February 2010.
3. Biowapens, de dodelijke kant van levenswetenschap. <http://www.kennislink.nl/publicaties/biowapens-de-dodelijke-kant-van-levenswetenschap>. Accessed July 16, 2013.

4. van Asselt M, de Vries P, van Aanholt J. Onzekere toekomsten in de Nationale Risicobeoordeling (NRB) [unsure futures in the national risk assessment (NRA)], article in the Dutch Magazine for National Security and Crisismanagement, February 2013.
5. Wetenschappelijke Raad voor het Regeringsbeleid (WRR) Evenwichtskunst: Over de verdeling van verantwoordelijkheid voor fysieke veiligheid. *Den Haag* 2010:42.
6. Minister of the Interior and Kingdom Relations, National Security (letter to Parliament), February 22, 2010, TK 2009-2010, 30821 nr. 10.
7. Minister of Security and Justice, National Security (letter to Parliament), June 5, 2012, TK 2009-2010, 30821 nr. 16.

*Manuscript received December 19, 2012;
accepted for publication May 17, 2013.*

Address correspondence to:
Maaïke van Tuyll
Ministry of Security and Justice
National Coordinator for Security and Counterterrorism (NCTV)
P.O. Box 16950
The Hague 2500 BZ
The Netherlands
E-mail: m.c.van.tuyll@nctv.minvenj.nl