COURSE CODE	BIRD 315
COURSE NAME	GLOBLE CHANGE AND SECURITY

GLOBLE CHANGE AND SECURITY

International relations, is a branch of political science. It represents the study of foreign affairs and global issues among states within the **international system**, including the roles of states, international organizations (IGOs), non-governmental organizations (NGOs), and multinational corporations (MNCs).

United Nations

The **United Nations** (**UN**) is an international organization that describes itself as a "global association of governments facilitating co-operation in international law, international security, economic development, and social equity"; It is the most prominent international institution. Many of the legal institutions follow the same organisational structure as the UN.

Economic institutions

- World Trade Organisation
- World Bank
- International Monetary Fund
- asim Asian Development Bank

International legal bodies

Human rights

- United Nations Human Rights Council
- Human Rights Committee
- European Court of Human Rights
- Inter-American Court of Human Rights
- International Criminal Tribunal for Rwanda
- International Criminal Tribunal for the Former Yugoslavia
- International Criminal Court

Legal

- International Court of Justice
- European Court of Justice
- African Court of Justice
- International Tribunal for the Law of the Sea

Global Change, Peace & Security

September 11 and its aftermath have dramatised one of the distinguishing trends of our time: *the globalisation of insecurity.* These extraordinary events have served to remind us of the sheer scale and complexity of contemporary change.

Global Change, Peace & Security is a leading refereed journal that addresses the difficult practical and theoretical questions posed by a rapidly globalising world. By focusing on the international dimension of political, economic and cultural life, it cuts across the traditional boundaries that separate states, economies and societies, as well as disciplines and ideologies.

Global Change, Peace & Security seeks to illuminate the sharp and often perplexing contradictions of an increasingly integrated yet fragmented world. Ethno-nationalism, the break-up of established states, and religious and civilizational divisions coexist with new forms of economic and financial integration. Gross violations of human rights, environmental degradation, large and uncontrolled population movements, and rapidly expanding transnational crime are taking place at a time of unparalleled UN activism, and the rise of a host of new legal and institutional arrangements, both regionally and globally.

Global Change, Peace & Security aims to explore these trends and counter-trends. It endeavours to foster a more holistic interpretation of the dichotomy of competitive geopolitics and geoconomics on the one hand and emerging conceptions of common, comprehensive and human security on the other.It analyses the sources and consequences of conflict, violence and insecurity, but also the conditions and prospects for conflict transformation, peacekeeping and peace-building.

Global Change, Peace & Security intends to bring to this task the insights of diverse cultural and intellectual traditions, not least the increasingly influential and diverse perspectives of the Asia-Pacific region. Its aim is to contribute to a scholarly and cosmopolitan dialogue on the nature, origins and remedies of the contemporary human predicament.

Peer Review: ***Global Change, Peace & Security*** is internationally refereed. Submissions are refereed by specialists in the field for originality, structural integrity and factual accuracy. An editorial review, referee reports and the author's response to these reports form the basis of the decision whether to publish submitted articles. All decisions of the Editors are final.

Views expressed in articles and communications do not reflect the opinion of the Editorial Committee or the Editors. Communications in ***Global Change, Peace & Security*** are reflective opinion pieces and the Editorial Committee welcomes diverse perspectives on contemporary issues.

Disclaimer

Food Security and Global Change

In recent years, the challenge of ensuring that our food system remains safe and secure has gained significant attention. Driven by concerns over hunger and insecurity caused by rising food prices and high profile events of food system contamination including spinach, pet food and peanut butter, experts, policymakers, the media and the public are asking hard questions about the implication of processes of global change on our increasingly global food networks.

In today's changing and globalized world, food insecurity is not just hunger. Food insecurity continues to impact billions of people on a daily basis and solving this problem requires addressing malnutrition from undernourishment, nutrient deficiency, and overnutrition.

Food security also requires ensuring that food supplies remain free from threats to human health whether from unintentional contamination (food safety) but also from intentional contamination by actors intent on using networked food systems to intentionally cause harm (food defense).

Sustainability will need to be a key core theme of food security efforts to ensure their long terms success. The environmental impacts of agriculture and food production are significant drivers of processes of global change. Agriculture and food production will experience significant impacts as a result of those processes and efforts to develop a more sustainable global food system are central to addressing global change processes through mitigating effects and helping people adapt impacts.

CUSA's research program on food security examines the evolving landscape of challenges to the security, safety and sustainability of the global food systems and identifies ways to manage threats and reduce vulnerabilities to help ensure people have access to the sufficient, safe and nutritious food necessary to lead active and healthy lives.

Food security
Growth in food production has been greater than population growth. Food per person increased during the 1961-2005 period. The y-axis is percent of 1999-2001 average food production per capita. Data source: World Resources Institute.

Food security refers to the availability of food and one's access to it. A household is considered food secure when its occupants do not live in hunger or fear of starvation. According to the World Resources Institute, global per capita food production has been increasing substantially for the past several decades. In 2006, MSNBC reported that globally, the number of people who are overweight has surpassed the number who are undernourished - the world had more than one billion people who were overweight, and an estimated 800 million who were undernourished. According to a 2004 article from the BBC, China, the world's most populous country, is suffering from an obesity epidemic. In India, the second-most populous country in the world, 30 million people have been added to the ranks of the hungry since the mid-1990s and 46% of children are underweight.

Worldwide around 852 million people are chronically hungry due to extreme poverty, while up to 2 billion people lack food security intermittently due to varying degrees of poverty (source: FAO, 2003). Six million children die of hunger every year - 17,000 every day. As of late 2007, increased farming for use in biofuels, world oil prices at more than $100 a barrel, global population growth, climate change, loss of agricultural land to residential and industrial development, and growing consumer demand in China and India have pushed up the price of grain. Food riots have recently taken place in many countries across the world

It is becoming increasingly difficult to maintain food security in a world beset by a confluence of "peak" phenomena, namely peak oil, peak water, peak phosphorus, peak grain and peak fish. More than half of the planet's population, numbering approximately 3.3 billion people, live in urban areas as of November 2007. Any disruption to farm supplies may precipitate a uniquely urban food crisis in a relatively short time. The ongoing global credit crisis has affected farm credits, despite a boom in commodity prices. Food security is a complex topic, standing at the intersection of many disciplines.

A new peer-reviewed journal of *Food Security: The Science, Sociology and Economics of Food Production and Access to Food* began publishing in 2009. In developing countries, often 70% or more of the population lives in rural areas. In that context, agricultural development among smallholder farmers and landless people provides a livelihood for people allowing them the opportunity to stay in their communities. In many areas of the world, land ownership is not available, thus, people who want or need to farm to make a living have little incentive to improve the land.

In the US, there are approximately 2,000,000 farmers, less than 1% of the population. A direct relationship exists between food consumption levels and poverty. Families with the financial resources to escape extreme poverty rarely suffer from chronic hunger; while poor families not only suffer the most from chronic hunger, but are also the segment of the population most at risk during food shortages and famines.

Two commonly used definitions of food security come from the UN's Food and Agriculture Organization (FAO) and the United States Department of Agriculture (USDA):

- Food security exists when all people, at all times, have physical and economic access to sufficient, safe and nutritious food to meet their dietary needs and food preferences for an active and healthy life. (FAO)
- Food security for a household means access by all members at all times to enough food for an active, healthy life. Food security includes at a minimum (1) the ready availability of nutritionally adequate and safe foods, and (2) an assured ability to acquire acceptable foods in socially acceptable ways (that is, without resorting to emergency food supplies, scavenging, stealing, or other coping strategies). (USDA)

The stages of food insecurity range from food secure situations to full-scale famine. "Famine and hunger are both rooted in food insecurity. Food insecurity can be categorized as either chronic or transitory. Chronic food insecurity translates into a high degree of vulnerability to famine and hunger; ensuring food security presupposes elimination of that vulnerability. [Chronic] hunger is not famine. It is similar to undernourishment and is related to poverty, existing mainly in poor countries."

Stunting and chronic nutritional deficiencies

Many countries experience perpetual food shortages and distribution problems. These result in chronic and often widespread hunger amongst significant numbers of people. Human populations respond to chronic hunger and malnutrition by decreasing body size, known in medical terms as stunting or stunted growth. This process starts *in utero* if the mother is malnourished and continues through approximately the third year of life. It leads to higher infant and child mortality, but at rates far lower than during famines. Once stunting has occurred, improved nutritional intake later in life cannot reverse the damage. Stunting itself is viewed as a coping mechanism, designed to bring body size into alignment with the calories available during adulthood in the location where the child is born. Limiting body size as a way of adapting to low levels of energy (calories) adversely affects health in three ways:

- Premature failure of vital organs occurs during adulthood. For example a 50 year old individual might die of heart failure because his/her heart suffered structural defects during early development.
- Stunted individuals suffer a far higher rate of disease and illness than those who have not undergone stunting.
- Severe malnutrition in early childhood often leads to defects in cognitive development.

"The analysis ... points to the misleading nature of the concept of subsistence as Malthus originally used it and as it is still widely used today. Subsistence in not located at the edge of a nutritional cliff, beyond which lies demographic disaster. Rather than one level of subsistence, there are numerous levels at which a population and a food supply can be in equilibrium in the sense that they can be indefinitely sustained. However, some levels will have smaller people and higher normal mortality than others."

Global water crisis

Grain storage facilities in Australia

Water deficits, which are already spurring heavy grain imports in numerous smaller countries, may soon do the same in larger countries, such as China or India. The water tables are falling in scores of countries (including Northern China, the US, and India) due to widespread overpumping using powerful diesel and electric pumps. Other countries affected include Pakistan, Afghanistan, and Iran. This will eventually lead to water scarcity and cutbacks in grain harvest. Even with the overpumping of its aquifers, China is developing a grain deficit. When this happens, it will almost certainly drive grain prices upward. Most of the 3 billion people projected to be added worldwide by mid-century will be born in countries already experiencing water shortages. After China and India, there is a second tier of smaller countries with large water deficits—Afghanistan, Algeria, Egypt, Iran, Mexico, and Pakistan. Four of these already import a large share of their grain. Only Pakistan remains self-sufficient. But with a population expanding by 4 million a year, it will also likely soon turn to the world market for grain.

Land degradation

Intensive farming often leads to a vicious cycle of exhaustion of soil fertility and decline of agricultural yields. Approximately 40% of the world's agricultural land is seriously degraded. In Africa, if current trends of soil degradation continue, the continent might be able to feed just 25% of its population by 2025, according to UNU's Ghana-based Institute for Natural Resources in Africa.

Land deals

Rich governments and corporations are buying up the rights to millions of hectares of agricultural land in developing countries in an effort to secure their own long-term food supplies. The head of the Food and Agriculture Organisation (FAO), Jacques Diouf, has warned that the controversial rise in land deals could create a form of "neocolonialism", with poor states producing food for the rich at the expense of their own hungry people. The South Korean firm Daewoo Logistics has secured a large piece of farmland in Madagascar to grow maize and crops for biofuels. Libya has secured 250,000 hectares of Ukrainian farmland, and China has begun to explore land deals in Southeast Asia.[32] Oil-rich Arab investors, including the sovereign wealth funds, are looking into Sudan, Ethiopia, Ukraine, Kazakhstan, Pakistan, Cambodia and Thailand.[33]

Some countries are using the acquisition of land for agriculture in return for other gains. Egypt is seeking land acquisition in Ukraine in exchange for access to its natural gas. Qatar has plans to lease 40,000 hectares of agricultural land along Kenya's coast to grow fruit and vegetables, in return for building a £2.4 billion port close to the Indian Ocean tourist island of Lamu.

Agriculture

According to a UN climate report, the Himalayan glaciers that are the principal dry-season water sources of Asia's biggest rivers - Ganges, Indus, Brahmaputra, Yangtze, Mekong, Salween and Yellow - could disappear by 2035 as temperatures rise. Approximately 2.4 billion people live in the drainage basin of the Himalayan rivers. India, China, Pakistan, Afghanistan, Bangladesh, Nepal and Myanmar could experience floods followed by severe droughts in coming decades. In India alone, the Ganges provides water for drinking and farming for more than 500 million people. The west coast of North America, which gets much of its water from glaciers in mountain ranges such as the Rocky Mountains and Sierra Nevada, also would be affected. Glaciers aren't the only worry that the developing nations have, sea level is also reported to rise as climate changes progresses, reducing the amount of land available for agriculture.

In other parts of the world a big effect will be low yields of grain according to the World Food Trade Model, specifically in the low latitude regions where much of the developing world is located. From this the price of grain will rise, along with the developing nations trying to grow the grain. Due to this, every 2-2.5% price hike will increase the number of hungry people 1%. And low crop yields is just one of the problem facing farmers in the low latitudes and tropical regions. The timing and length of the growing seasons, when farmers plant their crops, are going to be changing dramatically, per the USDA, due to unknown changes in soil temperature and moisture conditions.

Children

On 2008-04-29, a UNICEF UK report found that the world's poorest and most vulnerable children are being hit the hardest by the impact of climate change. The report, "Our Climate, Our Children, Our Responsibility: The Implications of Climate Change for the World's Children," says access to clean water and food supplies will become more difficult, particularly in Africa and Asia.

Watch the DIVERSEEDS short films on ways to fight wheat rust using crop wild relatives to improve resistance in modern varieties.

An epidemic of stem rust on wheat caused by race Ug99 is currently spreading across Africa and into Asia and is causing major concern. A virulent wheat disease could destroy most of the world's main wheat crops, leaving millions to starve. The fungus has spread from Africa to Iran, and may already be in Pakistan.[45][46][47]

The genetic diversity of the crop wild relatives of wheat can be used to improve modern varieties to be more resistant to rust. In their centers of origin wild wheat plants are screened for resistance to rust, then their genetic information is analysed and finally wild plants and modern varietes are crossed through means of modern plant breeding in order to transfer the resistance genes from the wild plants to the modern varieties.[48]

Dictatorship and kleptocracy

As the Nobel Prize-winning economist Amartya Sen has observed that "there is no such thing as an apolitical food problem." While drought and other naturally occurring events may trigger famine conditions, it is government action or inaction that determines its severity, and often even whether or not a famine will occur. The 20th century is full of examples of governments undermining the food security of their own nations–sometimes intentionally.

When governments come to power by force or rigged elections, and not by way of fair and open elections, their base of support is often narrow and built upon cronyism and patronage. Under such conditions "The distribution of food within a country is a political issue. Governments in most countries give priority to urban areas, since that is where the most influential and powerful families and enterprises are usually located. The government often neglects subsistence farmers and rural areas in general. The more remote and underdeveloped the area the less likely the government will be to effectively meet its needs. Many agrarian policies, especially the pricing of agricultural commodities, discriminate against rural areas. Governments often keep prices of basic grains at such artificially low levels that subsistence producers can not accumulate enough capital to make investments to improve their production.

Thus, they are effectively prevented from getting out of their precarious situation."

Further dictators and warlords have used food as a political weapon, rewarding their supporters while denying food supplies to areas that oppose their rule. Under such conditions food becomes a currency with which to buy support and famine becomes an effective weapon to be used against the opposition.

Governments with strong tendencies towards kleptocracy can undermine food security even when harvests are good. When government monopolizes trade, farmers may find that they are free to grow cash crops for export, but under penalty of law only able to sell their crops to government buyers at prices far below the world market price. The government then is free to sell their crop on the world market at full price, pocketing the difference. This creates an artificial "poverty trap" from which even the most hard working and motivated farmers may not escape.

When the rule of law is absent, or private property is non-existent, farmers have little incentive to improve their productivity. If a farm becomes noticeably more productive than neighboring farms, it may become the target of individuals well connected to the government. Rather than risk being noticed and possibly losing their land, farmers may be content with the perceived safety of mediocrity.

As pointed out by William Bernstein in his book *The Birth of Plenty*: "Individuals without property are susceptible to starvation, and it is much easier to bend the fearful and hungry to the will of the state. If a [farmer's] property can be arbitrarily threatened by the state, that power will inevitably be employed to intimidate those with divergent political and religious opinions."

Economic approaches

There are many economic approaches advocated to improve food security in developing countries. Three typical approaches are listed below. The first is typical of what is advocated by most governments and international agencies. The other two are more common to non-governmental organizations (NGO's).

Westernized view

Conventional thinking in westernized countries is that maximizing the farmers profit is the surest way of maximizing agricultural production; the higher a farmer's profit, the greater the effort that will be forthcoming, and the greater the risk the farmer is willing to take.

Place into the hands of farmers the largest number and highest quality tools possible (tools is used here to refer to improved production techniques,

improved seeds, secure land tenure, accurate weather forecasts, etc.) However, it is left to the individual farmer to pick and choose which tools to use, and how to use them, as farmers have intimate knowledge of their own land and local conditions.

As with other businesses, a percentage of the profits are normally reinvested into the business in the hopes of increasing production, and hence increase future profits. Normally higher profits translate into higher spending on technologies designed to boost production, such as drip irrigation systems, agriculture education, and greenhouses. An increased profit also increases the farmer's incentive to engage in double-cropping, soil improvement programs, and expanding usable area.

Food justice

Fight Hunger: Walk the World campaign is a United Nations World Food Programme initiative. An alternative view takes a collective approach to achieve food security. It notes that globally enough food is produced to feed the entire world population at a level adequate to ensure that everyone can be free of hunger and fear of starvation. That no one should live without enough food because of economic constraints or social inequalities is the basic goal.

This approach is often referred to as food justice and views food security as a basic human right. It advocates fairer distribution of food, particularly grain crops, as a means of ending chronic hunger and malnutrition. The core of the Food Justice movement is the belief that what is lacking is not food, but the political will to fairly distribute food regardless of the recipient's ability to pay.

Food sovereignty

A third approach is known as food sovereignty; though it overlaps with food justice on several points, the two are not identical. It views the business practices of multinational corporations as a form of neocolonialism. It contends that multinational corporations have the financial resources available to buy up the agricultural resources of impoverished nations, particularly in the tropics. They also have the political clout to convert these resources to the exclusive production of cash crops for sale to industrialized nations outside of the tropics, and in the process to squeeze the poor off of the more productive lands. Under this view subsistence farmers are left to cultivate only lands that are so marginal in terms of productivity as to be of no interest to the multinational corporations. Likewise, food sovereignty holds it to be true that communities should be able to define their own means of production and that food is a basic human right. With several multinational corporations now pushing agricultural technologies on developing countries, technologies that include improved seeds, chemical fertilizers, and pesticides, crop production has become an increasingly analyzed and debated issue. Many communities

calling for food sovereignty are protesting the imposition of Western technologies on to their indigenous systems and agency.

Those who hold a "food sovereignty" position advocate banning the production of most cash crops in developing nations, thereby leaving the local farmers to concentrate on subsistence agriculture. In addition, they oppose allowing low-cost subsidized food from industrialized nations into developing countries, what is referred to as "import dumping". Import dumping also happens by way of food aid distribution through programs like the USA's "Food for Peace" initiative.

World Food Summit

The World Food Summit was held in Rome in 1996, with the aim of renewing global commitment to the fight against hunger. The Food and Agriculture Organization of the United Nations (FAO) called the summit in response to widespread under-nutrition and growing concern about the capacity of agriculture to meet future food needs. The conference produced two key documents, the Rome Declaration on World Food Security and the World Food Summit Plan of Action.

The Rome Declaration calls for the members of the United Nations to work to halve the number of chronically undernourished people on the Earth by the year 2015. The Plan of Action sets a number of targets for government and non-governmental organizations for achieving food security, at the individual, household, national, regional and global levels.

AWorld Summit on Food Security

The World Summit on Food Security took place in Rome, Italy, between 16 and 18 November 2009. The decision to convene the summit was taken by the Council of FAO in June 2009, at the proposal of FAO Director-General Dr Jacques Diouf. Heads of State and Government attended the summit, which took place at the FAO’s headquarters.

Achieving food security

"The number of people without enough food to eat on a regular basis remains stubbornly high, at over 800 million, and is not falling significantly. Over 60% of the world's undernourished people live in Asia, and a quarter in Africa. The proportion of people who are hungry, however, is greater in Africa (33%) than Asia (16%). The latest FAO figures indicate that there are 22 countries, 16 of which are in Africa, in which the undernourishment prevalence rate is over 35%."[

In its "The State of Food Insecurity in the World 2003", FAO states that:]

> 'In general the countries that succeeded in reducing hunger were characterised by more rapid economic growth and specifically more rapid growth in their agricultural sectors. They also exhibited slower population growth, lower levels of HIV and higher ranking in the Human Development Index'.

As such, according to FAO, addressing agriculture and population growth is vital to achieving food security. Other organisations and people (eg Peter Singer, ...) too have come to this conclusion and advocate improvements in agriculture, and population control.

USAID proposes several key steps to increasing agricultural productivity which is in turn key to increasing rural income and reducing food insecurity. They include:

- Boosting agricultural science and technology. Current agricultural yields are insufficient to feed the growing populations. Eventually, the rising agricultural productivity drives economic growth.
- Securing property rights and access to finance.
- Enhancing human capital through education and improved health.
- Conflict prevention and resolution mechanisms and democracy and governance based on principles of accountability and transparency in public institutions and the rule of law are basic to reducing vulnerable members of society.

The UN Millennium Development Goals are one of the initiatives aimed at achieving food security in the world. In its list of goals, the first Millennium Development Goal states that the UN "is to eradicate extreme hunger and poverty", and that "agricultural productivity is likely to play a key role in this if it is to be reached on time".

"Of the eight Millennium Development Goals, eradicating extreme hunger and poverty depends on agriculture the most. (MDG 1 calls for halving hunger and poverty by 2015 in relation to 1990.)

Notably, the gathering of wild food plants appears to be an efficient alternative method of subsistence in tropical countries, which may play a role in poverty alleviation.[54]

The agriculture-hunger-poverty nexus

Eradicating hunger and poverty requires an understanding of the ways in which these two injustices interconnect. Hunger, and the malnourishment that accompanies it, prevents poor people from escaping poverty because it diminishes their ability to learn, work, and care for themselves and their family members. Food insecurity exists when people are undernourished as a result of

the physical unavailability of food, their lack of social or economic access to adequate food, and/or inadequate food utilization. Food-insecure people are those individuals whose food intake falls below their minimum calorie (energy) requirements, as well as those who exhibit physical symptoms caused by energy and nutrient deficiencies resulting from an inadequate or unbalanced diet or from the body's inability to use food effectively because of infection or disease. An alternative view would define the concept of food insecurity as referring only to the consequence of inadequate consumption of nutritious food, considering the physiological utilization of food by the body as being within the domain of nutrition and health. Malnourishment also leads to poor health hence individuals fail to provide for their families. If left unaddressed, hunger sets in motion an array of outcomes that perpetuate malnutrition, reduce the ability of adults to work and to give birth to healthy children, and erode children's ability to learn and lead productive, healthy, and happy lives. This truncation of human development undermines a country's potential for economic development–for generations to come.

There are strong, direct relationships between agricultural productivity, hunger, and poverty. Three-quarters of the world's poor live in rural areas and make their living from agriculture. Hunger and child malnutrition are greater in these areas than in urban areas. Moreover, the higher the proportion of the rural population that obtains its income solely from subsistence farming (without the benefit of pro-poor technologies and access to markets), the higher the incidence of malnutrition. Therefore, improvements in agricultural productivity aimed at small-scale farmers will benefit the rural poor first.

Increased agricultural productivity enables farmers to grow more food, which translates into better diets and, under market conditions that offer a level playing field, into higher farm incomes. With more money, farmers are more likely to diversify production and grow higher-value crops, benefiting not only themselves but the economy as a whole."[55]

Biotechnology for smallholders in the (sub)tropics

The area sown to genetically engineered crops in developing countries is rapidly catching-up with the area sown in industrial nations. According to the International Service for the Acquisition of Agri-biotech Applications (ISAAA), genetically engineered (biotech, GM) crops were grown by approximately 8.5 million farmers in 21 countries in 2005, up from 8.25 million farmers in 17 countries in 2004. The largest increase in biotech crop area in any country in 2005 was in Brazil, provisionally estimated at 44,000 km² (94,000 km² in 2005 compared with 50,000 km² in 2004). India had by far the largest year-on-year proportional increase, with almost a threefold increase from 5,000 km² in 2004 to 13,000 km² in 2005.

Current high regulatory costs imposed on varieties created by the more modern methods are a significant hurdle for development of genetically engineered crops well suited to developing country farmers by modern genetic methods. Once a new variety is developed, however, seed provides a good vehicle for distribution of improvements in a package that is familiar to the farmer.

Currently there are some institutes and research groups that have projects in which biotechnology is shared with contact people in less-developed countries on a non-profit basis. These institutes make use of biotechnological methods that do not involve high research and registration costs, such as conservation and multiplication of germplasm and phytosanitation.

Apart from genetic engineering, other forms of biotechnology also hold promise for enhancing food security. For instance, perennial rice is being developed in China, which could dramatically reduce the risk of soil erosion on upland smallholder farms.

Fossil fuel dependence

Further information: Agriculture and petroleum and Peak oil's effects on agriculture

While agricultural output increased as a result of the Green Revolution, the energy input into the process (that is, the energy that must be expended to produce a crop) has also increased at a greater rate, so that the ratio of crops produced to energy input has decreased over time. Green Revolution techniques also heavily rely on chemical fertilizers, pesticides and herbicides, some of which must be developed from fossil fuels, making agriculture increasingly reliant on petroleum products.

Between 1950 and 1984, as the Green Revolution transformed agriculture around the globe, world grain production increased by 250%. The energy for the Green Revolution was provided by fossil fuels in the form of fertilizers (natural gas), pesticides (oil), and hydrocarbon fueled irrigation.

David Pimentel, professor of ecology and agriculture at Cornell University, and Mario Giampietro, senior researcher at the National Research Institute on Food and Nutrition (INRAN), place in their study *Food, Land, Population and the U.S. Economy* the maximum U.S. population for a sustainable economy at 200 million. To achieve a sustainable economy and avert disaster, the United States must reduce its population by at least one-third, and world population will have to be reduced by two-thirds, says the study.

The authors of this study believe that the mentioned agricultural crisis will only begin to impact us after 2020, and will not become critical until 2050. The oncoming peaking of global oil production (and subsequent decline of

production), along with the peak of North American natural gas production will very likely precipitate this agricultural crisis much sooner than expected.[12] Geologist Dale Allen Pfeiffer claims that coming decades could see spiraling food prices without relief and massive starvation on a global level such as never experienced before.

However, one should take note that, (numbers taken from the CIA World Factbook), the country of Bangladesh achieved food self-sufficiency in 2002 with both a far higher population density than the USA (~1000 inhabitants per square kilometer in comparison to just 30/km^2 for the USA - so this is more than 30 times as many), and at only a tiny fraction of the USA's usage of oil, gas, and electricity. Also, pre-industrial Chinese mini-farmers/gardeners developed techniques to feed a population of more than 1000 people per square kilometer (cf. e.g. F.H. King's 1911 report, "Farmers of Forty Centuries"). Hence, the dominant problem is not energy availability but the need to stop and revert soil degradation.

Hybridization, genetic engineering and loss of biodiversity

In agriculture and animal husbandry, the green revolution popularized the use of conventional hybridization to increase yield by creating "high-yielding varieties". Often the handful of hybridized breeds originated in developed countries and were further hybridized with local varieties in the rest of the developing world to create high yield strains resistant to local climate and diseases. Local governments and industry have been pushing hybridization which has resulted in several of the indigenous breeds becoming extinct or threatened. Disuse because of unprofitability and uncontrolled intentional and unintentional cross-pollination and crossbreeding (genetic pollution), formerly huge gene pools of various wild and indigenous breeds have collapsed causing widespread genetic erosion and genetic pollution. This has resulted in loss of genetic diversity and biodiversity as a whole.[60]

A genetically modified organism (GMO) is an organism whose genetic material has been altered using the genetic engineering techniques generally known as recombinant DNA technology. Genetically Modified (GM) crops today have become a common source for genetic pollution, not only of wild varieties but also of other domesticated varieties derived from relatively natural hybridization.

Genetic erosion coupled with genetic pollution may be destroying unique genotypes, thereby creating a hidden crisis which could result in a severe threat to our **food security**. Diverse genetic material could cease to exist which would impact our ability to further hybridize food crops and livestock against more resistant diseases and climatic changes.

Genetic erosion in agricultural and livestock biodiversity

Genetic erosion in agricultural and livestock biodiversity is the loss of genetic diversity, including the loss of individual genes, and the loss of particular combinants of genes (or gene complexes) such as those manifested in locally adapted landraces of domesticated animals or plants adapted to the natural environment in which they originated. The term genetic erosion is sometimes used in a narrow sense, such as for the loss of alleles or genes, as well as more broadly, referring to the loss of varieties or even species. The major driving forces behind genetic erosion in crops are: variety replacement, land clearing, overexploitation of species, population pressure, environmental degradation, overgrazing, policy and changing agricultural systems.

The main factor, however, is the replacement of local varieties of domestic plants and animals by high yielding or exotic varieties or species. A large number of varieties can also often be dramatically reduced when commercial varieties (including GMOs) are introduced into traditional farming systems. Many researchers believe that the main problem related to agro-ecosystem management is the general tendency towards genetic and ecological uniformity imposed by the development of modern agriculture.

Price setting

On April 30, 2008 Thailand announces the project of the creation of the Organisation of Rice Exporting Countries with the potential to develop into a price-fixing cartel for rice.

Treating food the same as other internationally traded commodities

On October 23, 2008, Associated Press reported the following:

"Former President Clinton told a U.N. gathering Thursday [Oct 16, 2008] that the global food crisis shows "we all blew it, including me," by treating food crops "like color TVs" instead of as a vital commodity for the world's poor....Clinton criticized decades of policymaking by the World Bank, the International Monetary Fund and others, encouraged by the U.S., that pressured Africans in particular into dropping government subsidies for fertilizer, improved seed and other farm inputs as a requirement to get aid. Africa's food self-sufficiency declined and food imports rose. Now skyrocketing prices in the international grain trade—on average more than doubling between 2006 and early 2008—have pushed many in poor countries deeper into poverty."

Food is not a commodity like others. We should go back to a policy of maximum food self-sufficiency. It is crazy for us to think we can develop

countries around the world without increasing their ability to feed themselves.[68]

– Former US President Bill Clinton, *Speech at United Nations World Food Day, October 16, 2008*

Hai Vo wins Brower Youth Award

Hai Vo, a 2009 graduate of Social Ecology at UCI and a CUSA Student Research Associate, has been chosen as a winner of a 2009 Brower Youth Award. Hai co-founded the Real Food Challenge (RFC) at the University of California at Irvine (UCI) and worked with CUSA on a series of research, education and advocacy projects related to improving the sustainability of campus food systems.

In their citation of Hai, Earth Island Institute noted, "In order to educate and connect students, Hai co-organized events that brought students together to "simply eat," and to discuss their understanding of food. The RFC at UCI has engaged over 500 campus and community members in leadership development, networking convergences, dinners, roundtable events, educational series, and online networks, all centered around sustainable food systems." Earth Island Institute established the Brower Youth Awards in 2000 to honor founder and legendary environmental activist, David R. Brower and to call forth a new generation of leaders. Vo was be formally recognized for his efforts at the 10th Annual Brower Youth Awards on October 20, 2009 in San Francisco, California. Learn more about Hai and the other 2009 Brower Youth Award winners at Earth Island Institute's website.

Related Publications and Activities

Bryan McDonald presented "Food Security in an Age of Global Change" to the Paul Merage School of Business' Prosperitas group on January 28, 2010. Visit the Proseritas website to learn more about this event.

Bryan McDonald presented a paper on "Food Security and Global Environmental Change: Improving U.S. and Canadian Cooperation in the Face of Shared Threats and Vulnerabilities" to and interdisciplinary symposium on "Canadian Studies: On the Edge" held at the University of Southern California on October 9, 2009.

McDonald, Bryan L. and Richard A. Matthew. "Food Security in a Global Age: Addressing Challenges from Malnutrition, Food Safety and Environmental Change." Presented at the 2009 Annual Meeting of the American Political Science Association, Toronto, ON, Canada, September 3-6, 2009.

Bryan McDonald presented on "The Security of Food Production: What does the Future Hold?" as part of the 2008 California Alfalfa & Forage Symposium and Western Seed Conference held from December 2-4, 2008 in San Diego, California. This conference was organized by: UC Alfalfa & Forage Systems Workgroup, University of California Cooperative Extension, Western Alfalfa Seed Growers Association, University of Arizona Cooperative Extension.

CUSA presented a course on "Unconventional Security Issues" to the Osher Lifelong Learning Institute at UC, Irvine. The course, on October 14 and 21 included presentations by CUSA's Bryan McDonald about the changing landscape of security threats facing the United States including discussions about CUSA's work on food security.

Dr. Vandana Shiva presented the Center for Global Peace and Conflict Studies' 17th Annual Margolis Lecture on "The New Food Wars: Globalization, GMOs, and Biofuels." This speech on Wednesday, April 30, 2008 was supported by CUSA as part of our program of activities on food secuirty.

CUSA presented a course on "Unconventional Security Issues II" to the Osher Lifelong Learning Institute at UC, Irvine. The course, on April 17 and 24, included presentations by CUSA's Richard Matthew, Heather Goldsworthy, Bryan McDonald and Crystal Murphy Morgan on a range of issues including climate change, food security, terrorism, infectious disease, and microfinance and social entreprenuership.

CUSA took part in Focus the Nation: Sustainability and Climate Change Solutions at UCI on January 31, 2008. Part of a nationwide series of events, the Focus the Nation event at UC Irvine lays the foundation for a serious discussion about global warming solutions. CUSA related presentations included: Richard Matthew, "Climate Change, Peace and Conflict" and Bryan McDonald, "Climate Change, Sustainability and the Global Food System."

Bryan McDonald presented "Navigating the Changing Security Landscape"to the UC, Irvine Chancellor's Club on Tuesday, January 22, 2008. McDonald, who was a 2006-2007 Chancellor's Club Fellowship recipient, provided an overview of unconventional security issues and the changing security landscape in the context of two cases: (1) food safety and security, and (2) the growth of virtual worlds and cyber security challenges.

CUSA presented a course on "Unconventional Security Issues" to the Osher Lifelong Learning Institute at UC, Irvine. The course, on September 18 and 25, included lessons on a range of security issues including climate change, food security, terrorism, and infectious disease.

Bryan McDonald, "The Food System and Human Security: Confronting Hunger and Biological Threats in a Time of Global Change." Presented at 47th

International Studies Associationconvention, held March 22-25, 2006, in San Diego, California.

Richard Matthew and Bryan McDonald. "Cities Under Siege: Urban Planning and the Threat of Infectious Disease." *Journal of the American Planning Association (JAPA)* Vol. 72 No. 1 (Winter 2006): 109-117.

Bryan McDonald, "Human Security and Food Security in an Age of Transnational Threats,"Public Policy and Security Speaker Series, University of California, Los Angeles, May 10 2005.

Richard Matthew and Bryan McDonald. "Cities Under Siege: Transnational Threats and Urban Vulnerabilities." Presented at the American Planning Association's 2005 National Planning Conference, San Francisco, California., March 20, 2005.

Bryan McDonald, "Biotech Food, Biosecurity, and Changes in World Politics."Presented at the annual meeting of theAmerican Political Science Association, Chicago, Illinois, September 2-5, 2004.

Bryan McDonald, "From AgBioTech to AgBioTerror: Genetically Modified Food and International Security in the 21st Century." Presented at the annual meeting of The International Studies Association, Montreal, Canada, March 17-20, 2004.

Program Areas

Work at the SSRC is focused on four program areas, each of which supports working groups, conferences, grants and fellowships, and a wide range of other research activities: 1) Global Security and Cooperation; 2) Knowledge Institutions; 3) Migration; and 4) Renewing the Public. Examples of our work in each of these areas are provided below.

Global Security And Cooperation

The SSRC has a long-standing commitment to developing better understanding of problems of global security and cooperation, from work on arms control and nuclear proliferation, to emerging social, political, and religious movements, global public health challenges, and persistent forms of conflict and threats to human security. More recently, a significant portion of our work in this area clusters around the environment, building on the Council's decade-long "Global Environmental Change Program" as well as on our staff capacities in East Asia.

Examples of current program activity in this area include:

- Conflict Prevention and Peace Forum (CPPF), working to strengthen the knowledge base and analytical capacity of the United Nations system by providing UN staff with systematic channels of access to scholars, experts and practitioners outside the intergovernmental system. In 2008, CPPF engaged with some 23 countries and conflict situations in Africa, Asia and Latin America.

- HIV/AIDS Program, engaging government, non-governmental, and multilateral policy makers, as well as practitioners, in discussions on the global politics of AIDS, while also tackling methodological issues relating to sexual violence and conflict and HIV/AIDS.

- Gender and Security Program, an offshoot of our work on HIV/AIDS that is helping to advance new research agendas relating to gender, conflict and security, and sexual violence.

- Project on HIV/AIDS in the Russian Federation, which recently completed its first phase.

- China Environment and Health Program, promoting the generation and dissemination of new, social science-based research on the relationship between health, environment, and development in China.

- Ongoing work on provincial health in Vietnam by the Vietnam Program.

- Inaugural CGP-SSRC Policy Forum, which explored measures for energy saving and reducing air pollution and CO2 emissions for use by local officials, activists, and other actors in mid-sized cities within developing Asian countries.

- American Human Development Project, which by gathering data on well-being for each of America's congressional districts turns the lens of human security on the United States.

- Alex de Waal's program on Sudan and Darfur as well as his initiatives on How Genocides End, the Epidemiology of Lethal Violence, and the Political Marketplace.

- Leon Sigal's Northeast Asia Security Project, which among other activities has been helping to facilitate visits to Pyongyang, North Korea, for Obama administration officials.

Knowledge Institutions

Technological, social, political, and economic conditions are changing the production of knowledge in contemporary societies. Traditional institutions of science and education are being transformed and new ones created. The SSRC works to understand these shifts and their implications. It affirms a commitment to rigorous social science that can inform public and private sectors on topics related to mounting challenges in public higher education, changing models of undergraduate and graduate training, new practices of scientific research, and emerging partnerships in K-12 education.

Examples of current program activity in this area include:

- Digital Media and Learning Program, examining the impacts of digital media on the learning practices and processes of social institutions like schools, libraries, museums, community centers, and science centers.

- Future of Science Program, assessing the effectiveness of NSF-sponsored programs that have been designed to prepare graduate students in the sciences for collaborative interdisciplinary research.

- Education Research Program, dedicated to the promotion of rigorous social science research on education. Recent intiatives have included incubating a Research Alliance on New York City Schools, leading a longitudinal study on the effectiveness of higher education for America's underserved populations, and initiating a major cross-national study of school discipline and its impact on student performance.

Migration

International migration is at historically high levels. Enormous movements of people are changing the demographic composition of host and sending societies, with profound implications for economic, cultural and political life. The SSRC organizes and sponsors research on migration that focuses both on the experiences of individual nations and localities and on the comparative and collaborative dimensions of immigration across nations and regions.

The SSRC's Migration Program has led our work in this area since 1994. Its recent work focuses on:

- Migration and Development, helping researchers and practitioners to better understand how migration and development affect one another.

- Migration and Religion, bringing together scholars to explore the interrelationship between religion and settlement in new societies.

- Migration and Education, studying the educational needs of immigrant and second generation students.

- Diaspora-Government Relations, working to determine how members of diasporas and the U.S. government seek to influence one another in attaining goals having to do with migrants' homelands.

Renewing The Public

The "public" is distinct from community or even civil society in general. Publics connect people who are not in the same families, communities, and clubs– people who are not the same as each other. As such, they are central to the functioning of modern societies. What are the forms, locations, and conditions of public life? How do publics work, how are they supported by different kinds of physical and virtual communicative spaces, how do they figure in political and cultural life? For several years, the SSRC's work in this area centers on the parts played by media and religion in fostering a democratic public sphere, on public and private responses to risk and catastrophe, and on public issues in urban development. Moving forward, we are pursuing projects related to President Obama's efforts to make the government a more effective provider of public services and a more effective partner to private organizations that pursue the public good. See Craig Calhoun's recent essay, "Remaking America: Public Institutions and the Public Good."

Examples of current program activity in this area include:

- The Transformations of the Public Sphere essay forum and Public Sphere Guide, resources for the renewal of the public sphere.

- Necessary Knowledge for a Democratic Public Sphere Program, working to foster a stronger culture of collaboration among researchers, advocates, and activists working on policy and social change issues in media and communications.

- "Toward Detente in Media Piracy" Project, continuing a long line of SSRC work on intellectual property.

- Media Research Hub, designed to map relations among people, institutions, and resources within the media field.

- Religion and the Public Sphere Program, pursuing projects on religion and international affairs and on how spiritual practice shapes public life in the United States.

- Academia and the Public Sphere Grants Program, promoting public engagement by scholars who have specialized knowledge of Islamic traditions and Muslim communities.

- Privatization of Risk Project, seeking to advance work on the consequences of America having displaced risk from institutions and communities onto families.

- Learning from Katrina Project, mobilizing research on issues connected to the Katrina disaster and to similar events.

- Mixed Income Housing Research Design Project, addressing a significant lacuna in research literature on public housing in the United States.

Global Monitoring for Environment and Security

Global Monitoring for Environment and Security (**GMES**) is a joint initiative of the European Commission and European Space Agency, which aims at achieving an autonomous and operational Earth observation capacity.

The objective is to rationalize the use of multiple-sources data to get a timely and quality information, services and knowledge, and to provide autonomous and independent access to information in relation to environment and security. In other words, it will pull together all the information obtained by environmental satellites, air and ground stations to provide a comprehensive picture of the "health" of Earth.

Main users of GMES will be policy-makers. GMES should allow them to prepare national, European and international legislation on environmental matters (including climate change) and to monitor the implementation of this legislation.

GMES builds upon 4 pillars: the space component (observation satellites and associated ground segment with missions observing land, atmospheric and oceanographic parameters), in-situ measurements (ground-based and airborne data gathering networks providing information on oceans, continental surface and atmosphere), data harmonization and standardization, and services to users.

The geo-spatial information services offered by GMES can be grouped into six main interacting themes: land, ocean, emergency response, atmosphere, security and climate change. The first three GMES services under the land, ocean and emergency response themes and two additional services addressing the atmosphere and security themes were unveiled at the GMES Forum held in Lille in September 2008. Currently in their pre-operational phase, it is foreseen that these services enter into a EU-wide operational phase by 2011, with the objective to be fully operational by 2014.

GMES is fast moving towards an operational phase. The key to providing operational GMES services is to have an appropriate governance and business model structure in place which supports provisioning of these services.

GMES is the European Union contribution to the Global Earth Observation System of Systems GEOSS.

A brief history of GMES

19 May 1998: institutions involved in the development of space activities in Europe give birth to GMES through a declaration known as "The Baveno Manifesto". At that time, GMES stands for "Global Monitoring for Environmental Security"

Year 1999: the name is changed to "Global Monitoring for Environment and Security", thus illustrating that the management of the environment also has security implications.

Year 2001: at the occasion of the Gothenburg Summit, the Heads of State and Government request that "*the Community contribute to establishing by 2008 a European capacity for Global Monitoring for Environment and Security*".

October 2002: the nature and scope of the "Security" component of GMES are defined as addressing prevention of and response to crises related to natural and technological risk, humanitarian aid and international cooperation, monitoring of compliance with international treaties for conflict prevention, humanitarian and rescue tasks, peacekeeping tasks and surveillance of EU borders.

February 2004: the Commission Communication "*GMES: Establishing a GMES capacity by 2008*" introduces an Action Plan aimed at establishing a working GMES capacity by 2008. In 2004, a Framework Agreement is also signed between EC and ESA, thus providing the basis for a space component of GMES.

May 2005: the Commission Communication "*GMES: From Concept to Reality*" establishes priorities for the roll-out of GMES services in 2008, the initial focus

being on land monitoring, marine monitoring and emergency response services, also known as Fast Track Services (FTS). Later services, also known as Pilot Services, are expected to address atmosphere monitoring, security and climate change.

June 2006: the EC establishes the GMES Bureau, with the primary objective of ensuring the delivery of the priority services by 2008. Other objectives of the GMES Bureau are to address the issues of the GMES governance structure and the long-term financial sustainability of the system.

May 2007: adoption of the European Space Policy Communication, recognising GMES as a major flagship of the Space Policy.

September 2008: official launch of the 3 FTS services and 2 Pilot services in their pre-operational version at the occasion of the GMES Forum held in Lille, France.

November 2008: the Commission Communication "*GMES: We care for a Safer Planet*" establishes a basis for further discussions on the financing, operational infrastructure and effective management of GMES.

May 2009: the Commission Proposal for a Regulation on "*the European Earth Observation Programme (GMES) and its initial operations (2011-2013)*" proposes a legal basis for the GMES programme and EC funding of its initial operations.

From R&D to operational services

Over the last decades, European and national institutions have made substantial R&D efforts in the field of Earth observation. These efforts have resulted into tremendous achievements but the services and products developed during this period have limitations which are inherent to R&D activities (e.g. lack of service continuity on the long-term).

GMES has been conceived to move from R&D to operational services. The transition to operational services follows a phased approach:

- **2008 – 2010**: GMES pre-operational services (FTS and Pilot services)
- **2011 – 2013**: GMES initial operations
- **From 2014**: GMES fully operational services

The development of the five services is being realised by a series of projects launched by the European Commission and partly funded through the EU's 7th Framework Programme (FP7). These projects are geoland2 (land), MyOcean (marine), SAFER (emergency response), MACC (atmosphere) and G-MOSAIC (security).

- Geoland2 started on 1 September 2008. The project covers a wide range of domains such as land use, land cover change, soil sealing, water quality and availability, spatial planning, forest management, carbon storage and global food security.
- MyOcean started on 1 January 2009. It covers themes such as maritime security, oil spill prevention, marine resource management, climate change, seasonal forecast, coastal activities, ice survey and water pollution.
- SAFER started on 1 January 2009. The project addresses three main domains: civil protection, humanitarian aid and Security crises management.
- MACC started on 1 June 2009. The project will continue and refine the products developed in the projects GEMS and PROMOTE.
- G-MOSAIC started on 1 January 2009. Together with the LIMES project (partly funded by the European Commission under FP6), G-MOSAIC addresses domains such as maritime surveillance, critical infrastructure surveillance and support to peace-keeping operations.

Space missions

ESA is currently developing five types of new satellites called Sentinel to meet the needs of the GMES programme. The Sentinel missions include radar and super-spectral imaging for land, ocean and atmospheric monitoring. The Sentinel missions will have the following objectives:

- Sentinel 1 will provide all-weather, day and night radar imaging for land and ocean services. The first Sentinel-1 satellite is planned for launch at the end of 2011;
- Sentinel 2 will provide high-resolution optical imaging for land services (e.g. imagery of vegetation, soil and water cover, inland waterways and coastal areas). Sentinel-2 will also provide information for emergency services. The first Sentinel-2 satellite is planned for launch at the end of 2012;
- Sentinel 3 will provide ocean and global land monitoring services. The first Sentinel-3 satellite is planned for launch at the end of 2012;
- Sentinel-4, embarked as a payload upon a Meteosat Third Generation Satellite, will provide data for atmospheric composition monitoring. It will be launched in 2017;
- Sentinel-5 will also provide data for atmospheric composition monitoring. It will be embarked on a post-EUMETSAT Polar System (EPS) spacecraft and launched in 2019;
- Sentinel-6 is the intent to sustain high precision altimetry missions following the Jason-2 satellite.

Before the Sentinel missions provide data to GMES, numerous existing or planned space missions provide or will provide data useful to the provision of

GMES services. These missions are often referred to as "*GMES Contributing Missions (GCMs)*".

ERS: The European Remote Sensing Satellite ERS-1 (1991-2000) was ESA's first Earth observation satellite. ERS-2, launched in 1995, provides data related to ocean surface temperature, winds at sea and atmospheric ozone.

ENVISAT: Launched in 2002, Envisat is the largest Earth Observation spacecraft ever built. It carries sophisticated optical and radar instruments among which the Advanced Synthetic Aperture Radar (ASAR) and the Medium Resolution Imaging Spectrometer (MERIS). Envisat provides continuous observation and monitoring of the Earth's land, atmosphere, oceans and ice caps. ESA Member States have unanimously voted to extend the Envisat mission through to 2013.

Earth Explorers: Earth Explorers are smaller research missions dedicated to specific aspects of our Earth environment. Earth Explorer missions focus on the atmosphere, biosphere, hydrosphere, cryosphere and the Earth's interior with the overall emphasis on learning more about the interactions between these components and the impact that human activity is having on natural Earth processes. There are 6 missions selected for implementation:

- GOCE (Gravity Field and Steady-State Ocean Explorer), launched on 17 March 2009
- SMOS (Soil Moisture and Ocean Salinity), launched on 2 November 2009
- CryoSat-2 (measurement of the thickness of floating ice), scheduled for launch on 25 February 2010.
- Swarm (high-precision and high-resolution measurements of the strength and direction of the Earth's magnetic field), scheduled for launch in 2011
- ADM-Aeolus (Atmospheric Dynamics Mission), scheduled for launch in 2011
- EarthCARE (Earth Clouds, Aerosols and Radiation Explorer), scheduled for launch in 2013

MSG: the Meteosat Second Generation is a joint project between ESA and EUMETSAT.

MetOp: MetOp is Europe's first polar-orbiting satellite dedicated to operational meteorology. MetOp is a series of three satellites to be launched sequentially over 14 years from October 2006. The series will provide data for both operational meteorology and climate studies.

SPOT: SPOT (Satellite Pour l'Observation de la Terre) consists of a series of earth observation satellites providing high resolution images of the Earth.

SPOT-4 and SPOT-5 include sensors called VEGETATION able to monitor continental ecosystems.

TerraSAR-X: TerraSAR-X is a Earth observation satellite providing high quality topographic information. TerraSAR-X data have a wide range of applications (e.g. hydrology, meteorology, land use monitoring for agriculture, forest management and environmental protection)

COSMO-SkyMed: the COnstellation of small Satellites for the Mediterranean basin Observation is an Earth observation satellite system which will include four satellites equipped with synthetic aperture radar (SAR) sensors. Applications include seismic hazard analysis, environmental disaster monitoring and agricultural mapping.

DMC: The Disaster Monitoring Constellation (DMC) consists of five remote-sensing satellites. The constellation provides emergency Earth imaging for disaster relief under the International Charter for Space and Major Disasters.

JASON-2: The JASON-2 satellite provides precise measurements of ocean surface topography, surface wind speed and wave height; as this type of measurement is a crucial requirement for the GMES Marine Services the European Commission has included this type of mission in its latest communication on the future GMES Space Component as Sentinel 6

PLEIADES: The PLEIADES constellation consists of two satellites providing very high resolution images of the Earth

Data provided by non-European satellite missions (e.g. LANDSAT, GOSAT, RADARSAT) can also be used by GMES.

Other relevant initiatives

Other initiatives will also facilitate the development and functioning of GMES services:

- INSPIRE: this initiative aims at building a European spatial data infrastructure beyond national boundaries.
- Urban Atlas: Compiled from thousands of satellite photographs, the Urban Atlas provides detailed and cost-effective digital mapping, ensuring that city planners have the most up-to-date and accurate data available on land use and land cover. The Urban Atlas will enable urban planners to better assess risks and opportunities, ranging from threat of flooding and impact of climate change, to identifying new infrastructure and public transport needs. All cities in the EU will be covered by the Urban Atlas by 2011.

- SEIS: The Shared Environmental Information System (SEIS) is a collaborative initiative of the European Commission and the European Environment Agency (EEA) to establish together with the Member States an integrated and shared EU-wide environmental information system.

GMES is one of three related initiatives that are the subject of the GIGAS (*GEOSS, INSPIRE and GMES an Action in Support*) harmonization project under the auspices of the EU 7th Framework Programme.[1]

Environmental security

The Copenhagen School defines the referent object of environmental security as the environment as such, or some strategic part of the environment. [1]

Historically, the definition of international security has been debated extensively by political scientists and others, and has varied over time. After World War II, definitions typically focused on the subject of realpolitik that developed during the Cold War between the United States and the Soviet Union.

As tensions between the superpowers eased after the collapse of the Soviet Union, academic discussions of definitions of security significantly expanded to encompass a far broader range of threats to peace, including, particularly, environmental threats associated with the political implications of resource use or pollution. By the mid-1980s, this field of study was becoming known as "environmental security". Despite a wide range of semantic and academic debates over terms, it is now widely acknowledged that environmental factors play both direct and indirect roles in both political disputes and violent conflicts.

In the academic sphere environmental security is defined as the relationship between security concerns such as armed conflict and the natural environment. A small but rapidly developing field, it has become particularly relevant for those studying resource scarcity and conflict in the developing world. Prominent early researchers in the field include Felix Dodds, Norman Myers, Jessica Tuchman Mathews, Richard Ullman, Arthur Westing, Thomas Homer Dixon, Geoffrey Dabelko, Peter Gleick, and Joseph Romm.

The Millennium Project did a global assessment of the definitions of environmental security and created a synthesis definition: Environmental Security is environmental viability for life support, with three sub-elements:

- preventing or repairing military damage to the environment,
- preventing or responding to environmentally caused conflicts, and
- protecting the environment due to its inherent moral value.

Information security

The protection of data against unauthorized access. Programs and data can be secured by issuing passwords and digital certificates to authorized users. However, passwords only validate that a correct number has been entered, not that it is the actual person. Digital certificates and biometric techniques (fingerprints, eyes, voice, etc.) provide a more secure method (see authentication). After a user has been authenticated, sensitive data can be encrypted to prevent eavesdropping.

Authorized Users Can Be the Most Dangerous

Although precautions can be taken to authenticate users, it is much more difficult to determine if an authorized employee is doing something malicious. Someone may have valid access to an account for updating, but determining whether phony numbers are being entered requires a great deal more processing. The bottom line is that effective security measures are always a balance between technology and personnel management. See Parkerian hexad, information assurance, security scan, security audit, audit trail, NCSC, ICSA, access control, share-level security, user-level security and social engineering.

Face recognition is one of the best ways to authenticate a person. This TrueFace system from Miros uses neural network technology to distinguish a face with different appearances, such as with and without glasses and changing hair styles. (Image courtesy of Miros, Inc.)

Information security, often compressed to "infosec," is the preservation of secrecy and integrity in the storage and transmission of information. Whenever information of any sort is obtained by an unauthorized party, information security has been breached. Breaches of information security can be grouped into five basic classes: (1) interception of messages; (2) theft of stored data; (3) information sabotage (i.e., alteration or destruction of data belonging to another party); (4) spoofing (i.e., using stolen information to pose as somebody else); and (5) denial of service (i.e., deliberate shutdown of cash machines, electric-supply grids, air-traffic control networks, or the like). Individual computer experts ("hackers"), intelligence agencies, criminals, rival businesses, disgruntled employees, and other parties may all seek to breach information security. All these parties, plus law-abiding private individuals who wish to guard their privacy and protect themselves from identity theft, also have an interest in preserving information security.

Messages and secrets have been subject to interception and theft ever since the invention of writing, but the modern situation is especially challenging. Electronic storage, processing, and transmission of information are now ubiquitous in the developed world, creating novel vulnerabilities. People are authorized to withdraw cash or purchase products on the basis of a piece of

information (password or credit card number); trade secrets and business plans are electronically transmitted around the globe. In the U.S., over 95% of military and intelligence communications pass through network facilities owned by private carriers (e.g., the telephone system). Private speech may be broadcast locally by a mobile or cellular telephone or transmitted digitally over a network that can be tapped in numerous locations; databases full of confidential data reside in computers that can be accessed, perhaps illegally, by other computers communicating through networks; and so on. Information security—or insecurity—is a pervasive fact of modern life.

Consequently, breaching information security has become a common practice. For example, credit-card fraud costs approximately $20 per card per year. In 1994, an international criminal group used the Internet to penetrate Citicorp's computer system and shift $12 million from legitimate users' accounts to its own. Two ex-directors of the French in[1]telligence agency DGSE (Direction Generale de la Sécurité Extérieure) have confirmed that one of the agency's highest priorities is to spy on non-French corporations and business-related government agencies. United States government agencies such as the Office of the U.S. Trade Representative and high-tech companies such as Boeing, General Dynamics, Hughes Aircraft, and others have been specifically targeted by French espionage—and probably also by other organizations that happen to be less frank (or more prudent) in their public statements.

There are many tools for increasing information security, including software that scans for computer viruses or prevents unauthorized intrusions into computer systems from the networks; password systems of all sorts; physical access security for computers, discs, passcards, credit cards, and other objects containing sensitive information; and encryption of messages and of databases. While all these tools are important to the conduct of business by a large business or government department, passwords and encryption are probably the most important.

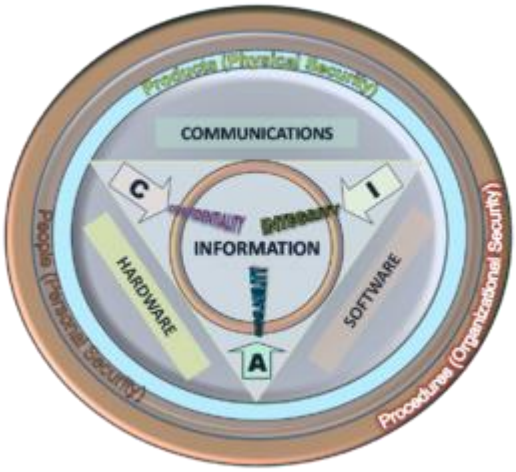
Passwords have the advantage of being simple to use. They are not, however, capable by themselves of providing a high level security for large numbers of users. First, most users are asked to supply passwords for many different systems: banking, shopping, e-mail, and so forth. This tempts users to choose short passwords (which are easier to remember but also easier to guess, therefore weaker) and to use the same password for more than one system (causing a domino effect if a password is guessed).

Cryptography—the process by which raw message information (*plaintext*) is mapped or *encrypted* to a scrambled form (*ciphertext*) before transmission or storage, then mapped back to its original form again (*decrypted*) when an authorized party wishes to read the plaintext—is arguably the ultimate tool of

information security. High-quality cryptographic systems that are breachable (if at all) only by resource-rich groups like the U.S. National Security Agency are widely available to businesses, governments, and private individuals. Appropriate cryptography can virtually guarantee the security of messages in transit and of information in databases; it can also, through "authentication," act as a super-password system whereby the identity of a would-be user (or information service supplier) can be positively confirmed. Cryptography has the disadvantages of added complexity, higher cost, and system slowdown.

Cryptography is also politically controversial, despite—or rather, because of—its technical power. Governments, corporations, private individuals, and private groups all have both legitimate and, occasionally, illegitimate motives for information security. Law-abiding persons and groups, or those rebelling against repressive laws, wish to be secure from surveillance by governments; criminals, terrorists, and the like also wish to be secure from surveillance by governments; government agents who are committing crimes wish to avoid public exposure; and so forth. It is generally advantageous to *all* parties, whether their activities are legitimate or illegitimate in whatever sense, to advocate maximum privacy for their own activities; it is generally advantageous to *governments* to advocate, in addition, maximum transparency for everyone else. Thus, for example, the U.S. government has sought (with little success) to prevent the spread of high-quality encryption algorithms, such as Pretty Good Privacy, outside the U.S., and inside the country has sought to establish voluntary compliance with "escrowed" cryptography systems. In such systems a government agency stores copies of cryptographic keys that enable it to decrypt communications between private parties using the system. In theory, these escrowed keys would be released to police or other government agents only when the court system had determined that there was a legitimate lawenforcement or national-security need to do so. Because such systems allow for third-party access to encrypted information by design, they are intrinsically less secure than a non-escrowed cryptography system, and therefore predictably unpopular with the private sector.

(DOD) The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC. See also communications security; computer security; information security; information system.



Information Security Components: or qualities, i.e., Confidentiality, Integrity and Availability (CIA). Information Systems are decomposed in three main portions, hardware, software and communications with the purpose to identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: Physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators)how to use products to ensure information security within the organizations.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.[1]

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their

employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. As a career choice there are many ways of gaining entry into the field. It offers many areas for specialization including: securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, to name a few.

History

Since the early days of writing, heads of state and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of written correspondence and to have some means of detecting tampering.

Julius Caesar is credited with the invention of the Caesar cipher c50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands.

World War II brought about many advancements in information security and marked the beginning of the professional field of information security.

The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through a network generically called the Internet or World Wide Web.

The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit.

The academic disciplines of computer security, information security and information assurance emerged along with numerous professional organizations - all sharing the common goals of ensuring the security and reliability of information systems.

Basic principles

Key concepts

For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA triad) as the core principles of information security. Many information security professionals firmly believe that Accountability should be added as a core principle of information security.

Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.

Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

Integrity

In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mis-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

In 2002, Donn Parker proposed an alternative model for the classic CIA triad that he called the six atomic elements of information. The elements are confidentiality, possession, integrity, authenticity, availability, and utility. The merits of the Parkerian hexad are a subject of debate amongst security professionals.

Authenticity

In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

Risk management

A comprehensive treatment of the topic of risk management is beyond the scope of this article. However, a useful definition of risk management will be

provided as well as some basic terminology and a commonly used process for risk management.

The CISA Review Manual 2006 provides the following definition of risk management: *"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."*[2]

There are two things in this definition that may need some clarification. First, the *process* of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerability emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). A **vulnerability** is a weakness that could be used to endanger or cause harm to an informational asset. A **threat** is anything (man made or act of nature) that has the potential to cause harm.

The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses (lost income, loss of life, loss of real property). It should be pointed out that it is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called *residual risk*.

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis may use quantitative analysis.

In broad terms the risk management process consists of:

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.
2. Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.

3. Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.
6. Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity.

For any given risk, Executive Management can choose to **accept the risk** based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to **mitigate the risk** by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be **transferred** to another business by buying insurance or out-sourcing to another business. The reality of some risks may be disputed. In such cases leadership may choose to **deny the risk**. This is itself a potential risk.[*citation needed*]

Controls

When Management chooses to mitigate a risk, they will do so by implementing one or more of three different types of controls.

Administrative

Administrative controls (also called procedural controls) consist of approved written policies, procedures, standards and guidelines. Administrative controls form the framework for running the business and managing people. They inform people on how the business is to be run and how day to day operations are to be conducted. Laws and regulations created by government bodies are also a type of administrative control because they inform the business. Some industry sectors have policies, procedures, standards and guidelines that must be followed - the Payment Card Industry (PCI) Data Security Standard required by Visa and Master Card is such an example. Other examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies.

Administrative controls form the basis for the selection and implementation of logical and physical controls. Logical and physical controls are manifestations of administrative controls. Administrative controls are of paramount importance.

Logical

Logical controls (also called technical controls) use software and data to monitor and control access to information and computing systems. For example: passwords, network and host based firewalls, network intrusion detection systems, access control lists, and data encryption are logical controls.

An important logical control that is frequently overlooked is the **principle of least privilege**. The principle of least privilege requires that an individual, program or system process is not granted any more access privileges than are necessary to perform the task. A blatant example of the failure to adhere to the principle of least privilege is logging into Windows as user Administrator to read Email and surf the Web. Violations of this principle can also occur when an individual collects additional access privileges over time. This happens when employees' job duties change, or they are promoted to a new position, or they transfer to another department. The access privileges required by their new duties are frequently added onto their already existing access privileges which may no longer be necessary or appropriate.

Physical

Physical controls monitor and control the environment of the work place and computing facilities. They also monitor and control access to and from such facilities. For example: doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks, etc. Separating the network and work place into functional areas are also physical controls.

An important physical control that is frequently overlooked is the **separation of duties**. Separation of duties ensures that an individual can not complete a critical task by himself. For example: an employee who submits a request for reimbursement should not also be able to authorize payment or print the check. An applications programmer should not also be the server administrator or the database administrator - these roles and responsibilities must be separated from one another.[3]

Security classification for information

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different

classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The type of information security classification labels selected and used will depend on the nature of the organisation, with examples being:

- In the business sector, labels such as: **Public, Sensitive, Private, Confidential**.
- In the government sector, labels such as: **Unclassified**, **Sensitive But Unclassified**, **Restricted**, **Confidential**, **Secret**, **Top Secret** and their non-English equivalents.
- In cross-sectoral formations, the Traffic Light Protocol, which consists of: **White, Green, Amber** and **Red**.

All employees in the organization, as well as business partners, must be trained on the classification schema and understand the required security controls and handling procedures for each classification. The classification a particular information asset has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place.

Access control

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected - the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with identification and authentication.

Identification is an assertion of who someone is or what something is. If a person makes the statement *"Hello, my name is John Doe."* they are making a claim of who they are. However, their claim may or may not be true. Before John Doe can be granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe.

Authentication is the act of verifying a claim of identity. When John Doe goes into a bank to make a withdrawal, he tells the bank teller he is John Doe (a claim of identity). The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has John Doe printed on it and compares the photograph on the license against the person claiming to be John Doe. If the photo and name match the person, then the teller has authenticated that John Doe is who he claimed to be.

There are three different types of information that can be used for authentication: **something you know, something you have, or something you are.** Examples of *something you know* include such things as a PIN, a password, or your mother's maiden name. Examples of *something you have* include a driver's license or a magnetic swipe card. *Something you are* refers to biometrics. Examples of biometrics include palm prints, finger prints, voice prints and retina (eye) scans. Strong authentication requires providing information from two of the three different types of authentication information. For example, something you know plus something you have. This is called two factor authentication.

On computer systems in use today, the Username is the most common form of identification and the Password is the most common form of authentication. Usernames and passwords have served their purpose but in our modern world they are no longer adequate. Usernames and passwords are slowly being replaced with more sophisticated authentication mechanisms.

After a person, program or computer has successfully been identified and authenticated then it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change). This is called **authorization**.

Authorization to access information and other computing services begins with administrative policies and procedures. The policies prescribe what information and computing services can be accessed, by whom, and under what conditions. The access control mechanisms are then configured to enforce these policies.

Different computing systems are equipped with different kinds of access control mechanisms - some may even offer a choice of different access control mechanisms. The access control mechanism a system offers will be based upon one of three approaches to access control or it may be derived from a combination of the three approaches.

The non-discretionary approach consolidates all access control under a centralized administration. The access to information and other resources is usually based on the individuals function (role) in the organization or the tasks the individual must perform. The discretionary approach gives the creator or owner of the information resource the ability to control access to those

resources. In the Mandatory access control approach, access is granted or denied basing upon the security classification assigned to the information resource.

Examples of common access control mechanisms in use today include Role-based access control available in many advanced Database Management Systems, simple file permissions provided in the UNIX and Windows operating systems, Group Policy Objects provided in Windows network systems, Kerberos, RADIUS, TACACS, and the simple access lists used in many firewalls and routers.

To be effective, policies and other security controls must be enforceable and upheld. Effective policies ensure that people are held **accountable** for their actions. All failed and successful authentication attempts must be logged, and all access to information must leave some type of audit trail.[*citation needed*]

Cryptography

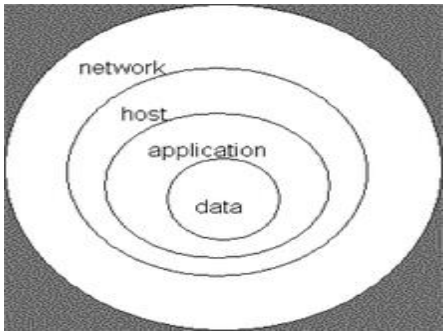
Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit (either electronically or physically) and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older less secure application such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using the WPA or WEP protocols. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GNUPG or PGP can be used to encrypt data files and Email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be

available when needed. PKI solutions address many of the problems that surround key management.

Defense in depth



Information security must protect information throughout the life span of the information, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its life time, information may pass through many different information processing systems and through many different parts of information processing systems. There are many different ways the information and information systems can be threatened. To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms. The building up, layering on and overlapping of security measures is called defense in depth. The strength of any system is no greater than its weakest link. Using a defence in depth strategy, should one defensive measure fail there are other defensive measures in place that continue to provide protection.

Recall the earlier discussion about administrative controls, logical controls, and physical controls. The three types of controls can be used to form the basis upon which to build a defense-in-depth strategy. With this approach, defense-in-depth can be conceptualized as three distinct layers or planes laid one on top of the other. Additional insight into defense-in- depth can be gained by thinking of it as forming the layers of an onion, with data at the core of the onion, people as the outer layer of the onion, and network security, host-based security and application security forming the inner layers of the onion. Both perspectives are equally valid and each provides valuable insight into the implementation of a good defense-in-depth strategy.

Process

The terms **reasonable and prudent person**, **due care** and **due diligence** have been used in the fields of Finance, Securities, and Law for many years. In recent years these terms have found their way into the fields of computing and information security. U.S.A. Federal Sentencing Guidelines now make it

possible to hold corporate officers liable for failing to exercise due care and due diligence in the management of their information systems.

In the business world, stockholders, customers, business partners and governments have the expectation that corporate officers will run the business in accordance with accepted business practices and in compliance with laws and other regulatory requirements. This is often described as the "reasonable and prudent person" rule. A prudent person takes due care to ensure that everything necessary is done to operate the business by sound business principles and in a legal ethical manner. A prudent person is also diligent (mindful, attentive, and ongoing) in their due care of the business.

In the field of Information Security, Harris[4] offers the following definitions of **due care** and **due diligence**:

"Due care are steps that are taken to show that a company has taken responsibility for the activities that take place within the corporation and has taken the necessary steps to help protect the company, its resources, and employees." And, [Due diligence are the] *"continual activities that make sure the protection mechanisms are continually maintained and operational."*

Attention should be made to two important points in these definitions. First, in due care, steps are taken to ***show*** - this means that the steps can be verified, measured, or even produce tangible artifacts. Second, in due diligence, there are **continual activities** - this means that people are actually doing things to monitor and maintain the protection mechanisms, and these activities are ongoing.

Change management

Change management is a formal process for directing and controlling alterations to the information processing environment. This includes alterations to desktop computers, the network, servers and software. The objectives of change management are to reduce the risks posed by changes to the information processing environment and improve the stability and reliability of the processing environment as changes are made. It is not the objective of change management to prevent or hinder necessary changes from being implemented.

Any change to the information processing environment introduces an element of risk. Even apparently simple changes can have unexpected effects. One of Managements many responsibilities is the management of risk. Change management is a tool for managing the risks introduced by changes to the information processing environment. Part of the change management process ensures that changes are not implemented at inopportune times when they

may disrupt critical business processes or interfere with other changes being implemented.

Not every change needs to be managed. Some kinds of changes are a part of the everyday routine of information processing and adhere to a predefined procedure, which reduces the overall level of risk to the processing environment. Creating a new user account or deploying a new desktop computer are examples of changes that do not generally require change management. However, relocating user file shares, or upgrading the Email server pose a much higher level of risk to the processing environment and are not a normal everyday activity. The critical first steps in change management are (a) defining change (and communicating that definition) and (b) defining the scope of the change system.

Change management is usually overseen by a Change Review Board composed of representatives from key business areas, security, networking, systems administrators, Database administration, applications development, desktop support and the help desk. The tasks of the Change Review Board can be facilitated with the use of automated work flow application. The responsibility of the Change Review Board is to ensure the organizations documented change management procedures are followed. The change management process is as follows:

- **Requested:** Anyone can request a change. The person making the change request may or may not be the same person that performs the analysis or implements the change. When a request for change is received, it may undergo a preliminary review to determine if the requested change is compatible with the organizations business model and practices, and to determine the amount of resources needed to implement the change.

- **Approved:** Management runs the business and controls the allocation of resources therefore, Management must approve requests for changes and assign a priority for every change. Management might choose to reject a change request if the change is not compatible with the business model, industry standards or best practices. Management might also choose to reject a change request if the change requires more resources than can be allocated for the change.

- **Planned:** Planning a change involves discovering the scope and impact of the proposed change; analyzing the complexity of the change; allocation of resources and, developing, testing and documenting both implementation and backout plans. Need to define the criteria on which a decision to back out will be made.

- **Tested:** Every change must be tested in a safe test environment, which closely reflects the actual production environment, before the change is applied to the production environment. The backout plan must also be tested.

- **Scheduled:** Part of the change review board's responsibility is to assist in the scheduling of changes by reviewing the proposed implementation date for potential conflicts with other scheduled changes or critical business activities.

- **Communicated:** Once a change has been scheduled it must be communicated. The communication is to give others the opportunity to remind the change review board about other changes or critical business activities that might have been overlooked when scheduling the change. The communication also serves to make the Help Desk and users aware that a change is about to occur. Another responsibility of the change review board is to ensure that scheduled changes have been properly communicated to those who will be affected by the change or otherwise have an interest in the change.

- **Implemented:** At the appointed date and time, the changes must be implemented. Part of the planning process was to develop an implementation plan, testing plan and, a back out plan. If the implementation of the change should fail or, the post implementation testing fails or, other "drop dead" criteria have been met, the back out plan should be implemented.

- **Documented:** All changes must be documented. The documentation includes the initial request for change, its approval, the priority assigned to it, the implementation, testing and back out plans, the results of the change review board critique, the date/time the change was implemented, who implemented it, and whether the change was implemented successfully, failed or postponed.

- **Post change review:** The change review board should hold a post implementation review of changes. It is particularly important to review failed and backed out changes. The review board should try to understand the problems that were encountered, and look for areas for improvement.

Change management procedures that are simple to follow and easy to use can greatly reduce the overall risks created when changes are made to the information processing environment. Good change management procedures improve the over all quality and success of changes as they are implemented. This is accomplished through planning, peer review, documentation and communication.

ISO/IEC 20000, The Visible OPS Handbook: Implementing ITIL in 4 Practical and Auditable Steps (Full book summary), and Information Technology Infrastructure Library all provide valuable guidance on implementing an efficient and effective change management program. information security

Business continuity

Business continuity is the mechanism by which an organization continues to operate its critical business units, during planned or unplanned disruptions that affect normal business operations, by invoking planned and managed procedures.

Unlike what most people think business continuity is not necessarily an IT system or process, simply because it is about the business. Today disasters or disruptions to business are a reality. Whether the disaster is natural or man-made (the TIME magazine has a website on the top 10), it affects normal life and so business. So why is planning so important? Let us face reality that "all businesses recover", whether they planned for recovery or not, simply because business is about earning money for survival.

The planning is merely getting better prepared to face it, knowing fully well that the best plans may fail. Planning helps to reduce cost of recovery, operational overheads and most importantly sail through some smaller ones effortlessly.

For businesses to create effective plans they need to focus upon the following key questions. Most of these are common knowledge, and anyone can do a BCP.

1. Should a disaster strike, what are the first few things that I should do? Should I call people to find if they are OK or call up the bank to figure out my money is safe? This is Emergencey Response. Emergency Response services help take the first hit when the disaster strikes and if the disaster is serious enough the Emergency Response teams need to quickly get a Crisis Management team in place.
2. What parts of my business should I recover first? The one that brings me most money or the one where I spend the most, or the one that will ensure I shall be able to get sustained future growth? The identified sections are the critical business units. There is no magic bullet here, no one answer satisfies all. Businesses need to find answers that meet business requirements.
3. How soon should I target to recover my critical business units? In BCP technical jargon this is called Recovery Time Objective, or RTO. This objective will define what costs the business will need to spend to recover from a disruption. For example, it is cheaper to recover a business in 1 day than in 1 hour.

4. What all do I need to recover the business? IT, machinery, records...food, water, people...So many aspects to dwell upon. The cost factor becomes clearer now...Business leaders need to drive business continuity. Hold on. My IT manager spent $200000 last month and created a DRP (Disaster Recovery Plan), whatever happened to that? a DRP is about continuing an IT system, and is one of the sections of a comprehensive Business Continuity Plan. Look below for more on this.
5. And where do I recover my business from... Will the business center give me space to work, or would it be flooded by many people queuing up for the same reasons that I am.
6. But once I do recover from the disaster and work in reduced production capacity, since my main operational sites are unavailable, how long can this go on. How long can I do without my original sites, systems, people? this defines the amount of business resilience a business may have.
7. Now that I know how to recover my business. How do I make sure my plan works? Most BCP pundits would recommend testing the plan at least once a year, reviewing it for adequacy and rewriting or updating the plans either annually or when businesses change.

Disaster recovery planning

While a business continuity plan (BCP) takes a broad approach to dealing with organizational-wide effects of a disaster, a disaster recovery plan (DRP), which is a subset of the business continuity plan, is instead focused on taking the necessary steps to resume normal business operations as quickly as possible. A disaster recovery plan is executed immediately after the disaster occurs and details what steps are to be taken in order to recover critical information technology infrastructure.[5]

Laws and regulations

*Below is a **partial** listing of European, United Kingdom, Canadian and USA governmental laws and regulations that have, or will have, a significant effect on data processing and information security. Important industry sector regulations have also been included when they have a significant impact on information security.*

- UK Data Protection Act 1998 makes new provisions for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The European Union Data Protection Directive (EUDPD) requires that all EU member must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.

- The Computer Misuse Act 1990 is an Act of the UK Parliament making computer crime (e.g. cracking - sometimes incorrectly referred to as

hacking) a criminal offence. The Act has become a model upon which several other countries including Canada and the Republic of Ireland have drawn inspiration when subsequently drafting their own information security laws.

- EU Data Retention laws requires Internet service providers and phone companies to keep data on every electronic message sent and phone call made for between six months and two years.
- The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232 g; 34 CFR Part 99) is a USA Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.

- Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the adoption of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. And, it requires health care providers, insurance providers and employers to safeguard the security and privacy of health data.
- Gramm-Leach-Bliley Act of 1999 (GLBA), also known as the Financial Services Modernization Act of 1999, protects the privacy and security of private financial information that financial institutions collect, hold, and process.

- Sarbanes-Oxley Act of 2002 (SOX). Section 404 of the act requires publicly traded companies to assess the effectiveness of their internal controls for financial reporting in annual reports they submit at the end of each fiscal year. Chief information officers are responsible for the security, accuracy and the reliability of the systems that manage and report the financial data. The act also requires publicly traded companies to engage independent auditors who must attest to, and report on, the validity of their assessments.
- Payment Card Industry Data Security Standard (PCI DSS) establishes comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

- State Security Breach Notification Laws (California and many others) require businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised, lost, or stolen.
- Personal Information Protection and Electronics Document Act (PIPEDA) - An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision ActThant is in fact the case.

Sources of standards

International Organization for Standardization (ISO) is a consortium of national standards institutes from 157 countries with a Central Secretariat in Geneva Switzerland that coordinates the system. The ISO is the world's largest developer of standards. The ISO-15443: "Information technology - Security techniques - A framework for IT security assurance", ISO-17799: "Information technology - Security techniques - Code of practice for information security management", ISO-20000: "Information technology - Service management", and ISO-27001: "Information technology - Security techniques - Information security management systems" are of particular interest to information security professionals.

The USA National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Department of Commerce. The NIST Computer Security Division develops standards, metrics, tests and validation programs as well as publishes standards and guidelines to increase secure IT planning, implementation, management and operation. NIST is also the custodian of the USA Federal Information Processing Standard publications (FIPS).

The Internet Society is a professional membership society with more than 100 organization and over 20,000 individual members in over 180 countries. It provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). The ISOC hosts the Requests for Comments (RFCs) which includes the Official Internet Protocol Standards and the RFC-2196 Site Security Handbook.

The Information Security Forum is a global nonprofit organization of several hundred leading organizations in financial services, manufacturing, telecommunications, consumer goods, government, and other areas. It provides research into best practice and practice advice summarized in its biannual

Standard of Good Practice, incorporating detail specifications across many areas.

The IT Baseline Protection Catalogs, or IT-Grundschutz Catalogs, ("IT Baseline Protection Manual" before 2005) are a collection of documents from the German Federal Office for Security in Information Technology (FSI), useful for detecting and combating security-relevant weak points in the IT environment ("IT cluster"). The collection encompasses over 3000 pages with the introduction and catalogs.

Professionalism

In 1989, Carnegie Mellon University established the Information Networking Institute, the United States' first research and education center devoted to information networking. The academic disciplines of computer security, information security and information assurance emerged along with numerous professional organizations during the later years of the 20th century and early years of the 21st century.

Entry into the field can be accomplished through self-study, college or university schooling in the field, or through week long focused training camps. Many colleges, universities and training companies offer many of their programs on- line. The GIAC-GSEC and Security+ certifications are both entry level security certifications. Membership of the Institute of Information Security Professionals (IISP) is gaining traction in the U.K. as the professional standard for Information Security Professionals.

The Certified Information Systems Security Professional (CISSP) is a mid- to senior-level information security certification. The Information Systems Security Architecture Professional (ISSAP), Information Systems Security Engineering Professional (ISSEP), Information Systems Security Management Professional (ISSMP), and Certified Information Security Manager (CISM) certifications are well-respected advanced certifications in information-security architecture, engineering, and management respectively.

Within the UK a recognised senior level information security certification is provided by CESG.

CLAS is the CESG Listed Adviser Scheme - a partnership linking the unique Information Assurance knowledge of CESG with the expertise and resources of the private sector.

CESG recognises that there is an increasing demand for authoritative Information Assurance advice and guidance. This demand has come as a result of an increasing awareness of the threats and vulnerabilities that information systems are likely to face in an ever-changing world.

The Scheme aims to satisfy this demand by creating a pool of high quality consultants approved by CESG to provide Information Assurance advice to government departments and other organisations who provide vital services for the United Kingdom.

CLAS consultants are approved to provide Information Assurance advice on systems processing protectively marked information up to, and including, SECRET. Potential customers of the CLAS Scheme should also note that if the information is not protectively marked then they do not need to specify membership of CLAS in their invitations to tender, and may be challenged if equally competent non-scheme members are prevented from bidding.

The profession of information security has seen an increased demand for security professionals who are experienced in network security auditing, penetration testing, and digital forensics investigation. In addition, many smaller companies have cropped up as the result of this increased demand in information security training and consulting.

Conclusion

Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review.

Bibliography

- Allen, Julia H. (2001). *The CERT Guide to System and Network Security Practices*. Boston, MA: Addison-Wesley. ISBN 0-201-73723-X.
- Krutz, Ronald L.; Russell Dean Vines (2003). *The CISSP Prep Guide* (Gold Edition ed.). Indianapolis, IN: Wiley. ISBN 0-471-26802-X.
- Layton, Timothy P. (2007). *Information Security: Design, Implementation, Measurement, and Compliance*. Boca Raton, FL: Auerbach publications. ISBN 978-0-8493-7087-8.
- McNab, Chris (2004). *Network Security Assessment*. Sebastopol, CA: O'Reilly. ISBN 0-596-00611-X.
- Peltier, Thomas R. (2001). *Information Security Risk Analysis*. Boca Raton, FL: Auerbach publications. ISBN 0-8493-0880-1.
- Peltier, Thomas R. (2002). *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. Boca Raton, FL: Auerbach publications. ISBN 0-8493-1137-3.
- White, Gregory (2003). *All-in-one Security+ Certification Exam Guide*. Emeryville, CA: McGraw-Hill/Osborne. ISBN 0-07-222633-1.

- Dhillon, Gurpreet (2007). *Principles of Information Systems Security: text and cases*. NY: John Wiley & Sons. ISBN 978-0471450566.